

## **EXHIBIT B, Part 2**

# **APPENDIX A**

**UNITED STATES DISTRICT COURT**  
**FOR THE DISTRICT OF MINNESOTA**

ROBERT KULLA, Derivatively on  
Behalf of TARGET CORPORATION,

Plaintiff,

v.

GREGG W. STEINHAFEL, BETH M.  
JACOB, JAMES A. JOHNSON,  
SOLOMON D. TRUJILLO, ANNE M.  
MULCAHY, ROXANNE S. AUSTIN,  
CALVIN DARDEN, MARY E.  
MINNICK, DERICA W. RICE, JOHN  
G. STUMPF, DOUGLAS M. BAKER,  
JR., HENRIQUE DE CASTRO, and  
KENNETH L. SALAZAR,

Defendants,

-and-

TARGET CORPORATION, a  
Minnesota corporation,

Nominal Defendant.

Case No. \_\_\_\_\_

**VERIFIED SHAREHOLDER  
DERIVATIVE COMPLAINT FOR  
BREACH OF FIDUCIARY DUTY  
AND WASTE OF CORPORATE  
ASSETS**

**DEMAND FOR JURY TRIAL**

### NATURE OF THE ACTION

1. This is a verified shareholder derivative action by plaintiff on behalf of nominal defendant Target Corporation ("Target" or the "Company") against certain of its officers and members of its Board of Directors (the "Board"). This action seeks to remedy defendants' violations of law, breaches of fiduciary duties, and waste of corporate assets that have caused substantial damages to the Company.

2. Target is the second largest general merchandise retailer in the United States. As part of its normal business practices, Target routinely collects its customers' personal and financial information, including credit and debit card numbers. Target assures its customers that it will protect this sensitive private information.

3. This action arises out of the Individual Defendants' (as defined herein) responsibility for the *second biggest data breach in retail history*. In violation of its express promise to do so, and contrary to reasonable customer expectations, Target failed to take reasonable steps to maintain its customers' personal and financial information in a secure manner. As a result of Target's complete and utter lack of appropriate security measures, thieves were able to steal sensitive personal and financial data from as many of *seventy million* customers who shopped at Target between November 27, 2013 and December 15, 2013, the height of the 2013 holiday season. For many of these victims, identity thieves have already utilized their personal information to commit fraud and other crimes. For tens of millions of others, constant vigilance of their financial and personal records will be required to protect themselves from the threat of having their identity stolen.



4. The Individual Defendants aggravated the damage to consumers from the data breach by failing to provide adequate and prompt notice to consumers and conveying a false sense of security to affected customers. In particular, the Individual Defendants allowed Target to delay acknowledging the breach to the public until December 19, 2013, over *three weeks* after the data breach began. Worse, Target disclosed the data breach only after third-party reports already broke the news. Even then, Target concealed the full nature and scope of the data breach. In particular, Target initially reported that the data breach affected forty million people and assured those affected by the data breach that "*the issue has been identified and eliminated,*" and that there was "*no indication that [personal identification number ("PIN")] numbers have been compromised.*" Target further reassured worried customers that "[s]omeone cannot visit an ATM with a fraudulent debit card and withdraw cash."

5. Despite these statements to the contrary, just days after Target's initial disclosure of the data breach, news outlets began reporting that encrypted PIN data had been stolen during the breach and that those codes could be used by thieves to make fraudulent withdrawals from the victims' bank accounts. In response to these allegations, Target continued to deny that any of its customers' PIN data had been compromised.

6. Then, on December 27, 2013, Target finally admitted that customers' PIN data had been compromised in the breach. Two weeks later, on January 10, 2014, Target released another statement indicating that the breach was far more significant than the Company had been reporting. In particular, Target disclosed that *seventy million*

customers may have been affected by the data breach, **30 million** more victims than Target previously reported.

7. The defendants' failures to implement any internal controls at Target designed to detect and prevent such a data breach, and then timely report it, have severely damaged Target. The Company's data breach is currently under investigation by the United States Secret Service ("Secret Service") and the Department of Justice ("DOJ"). Moreover, there are currently no less than **nine** class action lawsuits filed against Target on behalf of aggrieved customers. These class action lawsuits pose the risk of hundreds of millions of dollars in damages to the Company.

8. Plaintiff now brings this litigation on behalf of Target to rectify the conduct of the individuals bearing ultimate responsibility for the corporation's misconduct—the directors and senior management.

#### **JURISDICTION AND VENUE**

9. Jurisdiction is conferred by 28 U.S.C. §1332. Complete diversity among the parties exists and the amount in controversy exceeds \$75,000, exclusive of interest and costs.

10. This Court has jurisdiction over each defendant named herein because each defendant is either a corporation that conducts business in and maintains operations in this District, or is an individual who has sufficient minimum contacts with this District to render the exercise of jurisdiction by the District courts permissible under traditional notions of fair play and substantial justice.

11. Venue is proper in this Court in accordance with 28 U.S.C. §1391(a) because: (i) Target maintains its principal place of business in this District; (ii) one or more of the defendants either resides in or maintains executive offices in this District; (iii) a substantial portion of the transactions and wrongs complained of herein, including the defendants' primary participation in the wrongful acts detailed herein, and aiding and abetting and conspiracy in violation of fiduciary duties owed to Target, occurred in this District; and (iv) defendants have received substantial compensation in this District by doing business here and engaging in numerous activities that had an effect in this District.

### **THE PARTIES**

#### **Plaintiff**

12. Plaintiff Robert Kulla was a shareholder of Target at the time of the wrongdoing complained of, has continuously been a shareholder since that time, and is a current Target shareholder. Plaintiff is a citizen of Pennsylvania.

#### **Nominal Defendant**

13. Nominal defendant Target is a Minnesota corporation with principal executive offices located at 1000 Nicollet Mall, Minneapolis, Minnesota. Accordingly, Target is a citizen of Minnesota. Target serves guests at 1,921 stores including 1,797 in the United States and 124 in Canada. The Company operates through three reportable segments: the U.S. Retail segment, which includes all of Target's U.S. merchandising operations; the U.S. Credit Card segment, which offers credit to qualified guests through its branded proprietary credit cards; and the Canadian segment which includes costs incurred in the U.S. and Canada related to the 2013 Canadian retail market entry.

**Defendants**

14. Defendant Gregg W. Steinhafel ("Steinhafel") is Target's Chief Executive Officer ("CEO") and has been since May 2008; President and has been since August 1999; Chairman of the Board and has been since February 2009; and a director and has been since 2007. Defendant Steinhafel has been employed by Target since 1979. Defendant Steinhafel knowingly, recklessly, or with gross negligence: (i) caused or allowed the Company to conceal the full scope of the data breach, which affected at least seventy million customers; and (ii) failed to implement a system of internal controls to protect customers' personal and financial information. Target paid defendant Steinhafel the following compensation as an executive:

Fiscal Year	Salary	Stock Awards	Option Awards	Non-Equity Incentive Plan Compensation	Change in Pension Value and Nonqualified Deferred Compensation	Other Compensa- tion	Total
2012	\$1,500,000	\$5,285,245	\$5,248,573	\$2,860,000	\$665,528	\$5,068,118	\$20,547,464

Defendant Steinhafel is a citizen of Minnesota.

15. Defendant Beth M. Jacob ("Jacob") is Target's Chief Information Officer and has been since July 2008 and Executive Vice President, Target Technology Services and has been since January 2010. Defendant Jacob was also Senior Vice President, Target Technology Services from July 2008 to January 2010 and Vice President, Guest Operations, Target Financial Services from August 2006 to July 2008. Defendant Jacob knowingly, recklessly, or with gross negligence: (i) caused or allowed the Company to conceal the full scope of the data breach, which affected at least seventy million

customers; and (ii) failed to implement a system of internal controls to protect customers' personal and financial information. Defendant Jacob is a citizen of Minnesota.

16. Defendant James A. Johnson ("Johnson") is Target's Lead Independent Director and has been since at least April 2012 and a director and has been since 1996. Defendant Johnson is also a member of Target's Corporate Responsibility Committee and has been since at least April 2012. Defendant Johnson knowingly or recklessly: (i) caused or allowed the Company to conceal the full scope of the data breach, which affected at least seventy million customers; and (ii) failed to implement a system of internal controls to protect customers' personal and financial information. Target paid defendant Johnson the following compensation as a director:

<b>Fiscal Year</b>	<b>Fees Paid in Cash</b>	<b>Stock Awards</b>	<b>Option Awards</b>	<b>Change in Pension Value and Nonqualified Deferred Compensation</b>	<b>Total</b>
2012	\$135,000	\$90,055	\$71,477	\$13,174	\$309,706

Defendant Johnson is a citizen of Washington, D.C.

17. Defendant Solomon D. Trujillo ("Trujillo") is a Target director and has been since 1994. Defendant Trujillo is also Chairman of Target's Corporate Responsibility Committee and has been since at least April 2012. Defendant Trujillo knowingly or recklessly: (i) caused or allowed the Company to conceal the full scope of the data breach, which affected at least seventy million customers; and (ii) failed to implement a system of internal controls to protect customers' personal and financial information. Target paid defendant Trujillo the following compensation as a director:

<b>Fiscal Year</b>	<b>Fees Paid in Cash</b>	<b>Stock Awards</b>	<b>Option Awards</b>	<b>Change in Pension Value and Nonqualified Deferred Compensation</b>	<b>Total</b>
2012	\$105,000	\$90,055	\$71,477	\$32,165	\$298,697

Defendant Trujillo is a citizen of California.

18. Defendant Anne M. Mulcahy ("Mulcahy") is a Target director and has been since 1997. Defendant Mulcahy is also a member of Target's Audit Committee and has been since at least January 2014. Defendant Mulcahy knowingly or recklessly: (i) caused or allowed the Company to conceal the full scope of the data breach, which affected at least seventy million customers; and (ii) failed to implement a system of internal controls to protect customers' personal and financial information. Target paid defendant Mulcahy the following compensation as a director:

<b>Fiscal Year</b>	<b>Stock Awards</b>	<b>Total</b>
2012	\$275,003	\$275,003

Defendant Mulcahy is a citizen of Connecticut.

19. Defendant Roxanne S. Austin ("Austin") is a Target director and has been since 2002. Defendant Austin is also Chairman of Target's Audit Committee and has been since at least April 2012. Defendant Austin knowingly or recklessly: (i) caused or allowed the Company to conceal the full scope of the data breach, which affected at least seventy million customers; and (ii) failed to implement a system of internal controls to protect customers' personal and financial information. Target paid defendant Austin the following compensation as a director:

<b>Fiscal Year</b>	<b>Fees Paid in Cash</b>	<b>Stock Awards</b>	<b>Option Awards</b>	<b>Total</b>
2012	\$120,000	\$90,055	\$71,477	\$281,532

Defendant Austin is a citizen of California.

20. Defendant Calvin Darden ("Darden") is a Target director and has been since 2003. Defendant Darden is also a member of Target's Corporate Responsibility Committee and has been since at least January 2014. Defendant Darden knowingly or recklessly: (i) caused or allowed the Company to conceal the full scope of the data breach, which affected at least seventy million customers; and (ii) failed to implement a system of internal controls to protect customers' personal and financial information.

Target paid defendant Darden the following compensation as a director:

<b>Fiscal Year</b>	<b>Fees Paid in Cash</b>	<b>Stock Awards</b>	<b>Option Awards</b>	<b>Total</b>
2012	\$90,000	\$90,055	\$71,477	\$251,532

Defendant Darden is a citizen of Georgia.

21. Defendant Mary E. Minnick ("Minnick") is a Target director and has been since 2005. Defendant Minnick is also a member of Target's Audit Committee and Corporate Responsibility Committee and has been since at least April 2012. Defendant Minnick knowingly or recklessly: (i) caused or allowed the Company to conceal the full scope of the data breach, which affected at least seventy million customers; and (ii) failed to implement a system of internal controls to protect customers' personal and financial information. Target paid defendant Minnick the following compensation as a director:

<b>Fiscal Year</b>	<b>Stock Awards</b>	<b>Total</b>
2012	\$260,004	\$260,004

Defendant Minnick is a citizen of the United Kingdom.

22. Defendant Derica W. Rice ("Rice") is a Target director and has been since 2007. Defendant Rice is also a member of Target's Audit Committee and has been since at least April 2012. Defendant Rice knowingly or recklessly: (i) caused or allowed the Company to conceal the full scope of the data breach, which affected at least seventy million customers; and (ii) failed to implement a system of internal controls to protect customers' personal and financial information. Target paid defendant Rice the following compensation as a director:

<b>Fiscal Year</b>	<b>Stock Awards</b>	<b>Total</b>
2012	\$260,004	\$260,004

Defendant Rice is a citizen of Indiana.

23. Defendant John G. Stumpf ("Stumpf") is a Target director and has been since 2010. Defendant Stumpf was also a member of Target's Audit Committee from at least April 2012 to March 2013. Defendant Stumpf knowingly or recklessly: (i) caused or allowed the Company to conceal the full scope of the data breach, which affected at least seventy million customers; and (ii) failed to implement a system of internal controls to protect customers' personal and financial information. Target paid defendant Stumpf the following compensation as a director:

<b>Fiscal Year</b>	<b>Fees Paid in Cash</b>	<b>Stock Awards</b>	<b>Option Awards</b>	<b>Total</b>
2012	\$90,000	\$90,055	\$71,477	\$251,532

Defendant Stumpf is a citizen of California.

24. Defendant Douglas M. Baker, Jr. ("Baker") is a Target director and has been since March 2013. Defendant Baker was also a member of Target's Audit



Committee from March 2013 to at least April 2013. Defendant Baker knowingly or recklessly: (i) caused or allowed the Company to conceal the full scope of the data breach, which affected at least seventy million customers; and (ii) failed to implement a system of internal controls to protect customers' personal and financial information. Defendant Baker is a citizen of Minnesota.

25. Defendant Henrique De Castro ("De Castro") is a Target director and has been since March 2013. Defendant De Castro is also a member of Target's Corporate Responsibility Committee and has been since March 2013. Defendant De Castro knowingly or recklessly: (i) caused or allowed the Company to conceal the full scope of the data breach, which affected at least seventy million customers; and (ii) failed to implement a system of internal controls to protect customers' personal and financial information. Defendant De Castro is a citizen of California.

26. Defendant Kenneth L. Salazar ("Salazar") is a Target director and has been since July 2013. Defendant Salazar is also a member of Target's Corporate Responsibility Committee and has been since November 2013. Defendant Salazar knowingly or recklessly: (i) caused or allowed the Company to conceal the full scope of the data breach, which affected at least seventy million customers; and (ii) failed to implement a system of internal controls to protect customers' personal and financial information. Defendant Salazar is a citizen of Colorado.

27. The defendants identified in ¶¶14-15 are referred to herein as the "Officer Defendants." The defendants identified in ¶¶16-26 are referred to herein as the "Director

Defendants." Collectively, the defendants identified in ¶¶14-26 are referred to herein as the "Individual Defendants."

### **DUTIES OF THE INDIVIDUAL DEFENDANTS**

#### **Fiduciary Duties**

28. By reason of their positions as officers and directors of the Company, each of the Individual Defendants owed and owe Target and its shareholders fiduciary obligations of trust, loyalty, good faith, and due care, and were and are required to use their utmost ability to control and manage Target in a fair, just, honest, and equitable manner. The Individual Defendants were and are required to act in furtherance of the best interests of Target and not in furtherance of their personal interest or benefit.

29. To discharge their duties, the officers and directors of Target were required to exercise reasonable and prudent supervision over the management, policies, practices, and controls of the financial affairs of the Company. By virtue of such duties, the officers and directors of Target were required to, among other things:

(a) devise and maintain a system of internal controls sufficient to ensure that the Company's customers' personal and financial information is protected;

(b) ensure that the Company timely and accurately informed customers regarding any breach of their personal and financial information;

(c) conduct the affairs of the Company in an efficient, business-like manner in compliance with all applicable laws, rules, and regulations so as to make it possible to provide the highest quality performance of its business, to avoid wasting the Company's assets, and to maximize the value of the Company's stock; and

(d) remain informed as to how Target conducted its operations, and, upon receipt of notice or information of imprudent or unsound conditions or practices, make reasonable inquiry in connection therewith, and take steps to correct such conditions or practices.

#### **Breaches of Duties**

30. The conduct of the Individual Defendants complained of herein involves a knowing and culpable violation of their obligations as officers and directors of Target, the absence of good faith on their part, and a reckless disregard for their duties to the Company that the Individual Defendants were aware or reckless in not being aware posed a risk of serious injury to the Company.

31. The Individual Defendants, because of their positions of control and authority as officers and/or directors of Target, were able to and did, directly or indirectly, exercise control over the wrongful acts complained of herein. The Individual Defendants also failed to prevent the other Individual Defendants from taking such illegal actions. As a result, and in addition to the damage the Company has already incurred, Target has expended, and will continue to expend, significant sums of money.

#### **CONSPIRACY, AIDING AND ABETTING, AND CONCERTED ACTION**

32. In committing the wrongful acts alleged herein, the Individual Defendants have pursued, or joined in the pursuit of, a common course of conduct, and have acted in concert with and conspired with one another in furtherance of their common plan or design. In addition to the wrongful conduct herein alleged as giving rise to primary

liability, the Individual Defendants further aided and abetted and/or assisted each other in breaching their respective duties.

33. The Individual Defendants engaged in a conspiracy, common enterprise, and/or common course of conduct. During this time, the Individual Defendants failed to timely and accurately inform customers regarding the full scope of the breach of their personal and financial information.

34. The purpose and effect of the Individual Defendants' conspiracy, common enterprise, and/or common course of conduct was, among other things, to disguise the Individual Defendants' violations of law, breaches of fiduciary duty, and waste of corporate assets; and to conceal adverse information concerning the Company's operations.

35. The Individual Defendants accomplished their conspiracy, common enterprise, and/or common course of conduct by allowing the Company to purposefully or recklessly conceal the scope of the data breach affecting at least seventy million customers. Because the actions described herein occurred under the authority of the Board, each of the Individual Defendants was a direct, necessary, and substantial participant in the conspiracy, common enterprise, and/or common course of conduct complained of herein.

36. Each of the Individual Defendants aided and abetted and rendered substantial assistance in the wrongs complained of herein. In taking such actions to substantially assist the commission of the wrongdoing complained of herein, each Individual Defendant acted with knowledge of the primary wrongdoing, substantially

assisted in the accomplishment of that wrongdoing, and was aware of his or her overall contribution to and furtherance of the wrongdoing.

#### **BACKGROUND OF THE COMPANY AND ITS PRIVACY POLICY**

37. Target is the second largest general merchandise retailer in the United States. The Company operates 1,797 stores in the United States and 124 stores in Canada.

38. As stated in the Company's own "Privacy Policy," Target routinely collects personal information from its customers including a customer's name, mailing address, e-mail address, phone number, driver's license number, and credit/debit card number. In addition, when customers use their debit cards to make a purchase at Target, they are required to enter the PIN associated with their bank account. Target promises its customers that it will, among other things, *"maintain administrative, technical and physical safeguards to protect your personal information.* When we collect or transmit sensitive information such as a credit or debit card number, *we use industry standard methods to protect that information."*

#### **The Ramifications of Failing to Keep Customers' Data Secure Are Severe**

39. Notwithstanding its promise and duties to protect its customers' sensitive personal and financial information, Target allowed the sensitive and private information of tens of millions of its customers to be stolen. Target's failure to protect its customers' sensitive personal and financial information exposes victims to identity theft. Identity theft occurs when someone wrongfully obtains another's personal information without their knowledge to commit theft or fraud.

40. Armed with a person's personal and financial information, identity thieves can encode the victim's account information onto a different card with a magnetic strip creating a counterfeit card that can be used to make fraudulent purchases. With the addition of a victim's PIN, a thief can use the counterfeit card to withdraw money from that person's bank account.

41. Identity thieves can cause further damage to their victims by using personal information to open new credit and utility accounts, receive medical treatment on their health insurance, or even obtain a driver's license. Once a person's identity has been stolen, reporting, identifying, monitoring, and repairing the victim's credit is a cumbersome, expensive, and time-consuming process. In addition to the frustration of having to identify and close affected accounts, correct information in their credit reports, victims of identity theft often incur costs associated with defending themselves against civil litigation brought by creditors. Victims also suffer the burden of having difficulty obtaining new credit. Moreover, victims of identity theft must monitor their credit reports for future inaccuracies as fraudulent use of stolen personal information may persist for several years.

42. Annual monetary losses from identity theft are in the billions of dollars. According to The President's Identity Theft Task Force Report dated October 21, 2008, on identity theft produced in 2008:

In addition to the losses that result when identity thieves fraudulently open accounts or misuse existing accounts, ... individual victims often suffer indirect financial costs, including the costs incurred in both civil litigation initiated by creditors and in overcoming the many obstacles they face in obtaining or retaining credit. Victims of non-financial identity theft, for

example, health-related or criminal record fraud, face other types of harm and frustration.

In addition to out-of-pocket expenses that can reach thousands of dollars for the victims of new account identity theft, and the emotional toll identity theft can take, some victims have to spend what can be a considerable amount of time to repair the damage caused by the identity thieves. Victims of new account identity theft, for example, must correct fraudulent information in their credit reports and monitor their reports for future inaccuracies, close existing bank accounts and open new ones, and dispute charges with individual creditors.

43. The significant impact identity theft can have on consumers and the extreme financial ramification the failure to secure personal information can cause has led to the enactment of numerous privacy-related laws aimed toward protecting consumer information and disclosure requirements, including, for example: (i) Gramm-Leach-Bliley Act; (ii) Fair Credit Reporting Act; (iii) Fair and Accurate Credit Transactions Act; (iv) Federal Trade Commission Act, 15 U.S.C. §§41-58; (v) Driver's Privacy Protection Act; (vi) Health Insurance Portability and Accountability Act; (vii) The Privacy Act of 1974; (viii) Social Security Act Amendments of 1990; (ix) E-Government Act of 2002; and (x) Federal Information Security Management Act of 2002.

44. Moreover, the recent wave of cyber-attacks striking American corporations prompted warnings from federal officials, including one issued in May 2013 by the Department of Homeland Security. In particular, the warning was issued by an agency called ICS-Cert, which monitors attacks on computer systems that run industrial processes. The warning stated that the government was "highly concerned about hostility against critical infrastructure organizations."

45. The Individual Defendants were fully aware of the risk of a potential data breach. On August 27, 2007, Dr. Neal Krawetz, a data security expert working for Hacker Factor Solutions, publicly disclosed a white paper<sup>1</sup> titled "Point-of-Sale Vulnerabilities" (the "White Paper") warning Target about the possibility of a point-of-sale data breach. The White Paper used Target as an example of the potential ramifications of a point-of-sale data breach at a major retailer and estimated that as many as fifty-eight million card accounts could be compromised if Target's point-of-sale system was compromised.

46. Moreover, the Individual Defendants were fully aware of the ramifications of failing to keep customers' data secure and knew that the Company could be subject to costly government enforcement actions and private litigation. As stated in the risk disclosures in the Company's Annual Report on Form 10-K filed with the U.S. Securities and Exchange Commission ("SEC") on March 20, 2013:

*If we experience a significant data security breach or fail to detect and appropriately respond to a significant data security breach, we could be exposed to government enforcement actions and private litigation. In addition, our guests could lose confidence in our ability to protect their personal information, which could cause them to discontinue usage of REDcards, decline to use our pharmacy services, or stop shopping with us altogether. The loss of confidence from a significant data security breach involving team members could hurt our reputation, cause team member recruiting and retention challenges, increase our labor costs and affect how we operate our business.*

---

<sup>1</sup> A white paper is an authoritative report or guide helping readers to understand an issue, solve a problem, or make a decision. White papers are used in two main spheres: government and business-to-business marketing.



**THE INDIVIDUAL DEFENDANTS' FAILURE TO PROTECT CUSTOMERS' PERSONAL INFORMATION LEADS TO RECORD-SETTING DATA BREACH**

47. Target's data breach compromised seventy million customers' personal and financial data. Within days of the breach, millions of affected customers' financial and personal information was being sold on the black-market. Moreover, bank cards that had only been used at Target were found to have been used to make unauthorized purchases at Target stores.

48. News of the data breach first broke out on December 18, 2013, when KrebsOnSecurity.com, a website dedicated to reporting cybercrime, published an article indicating the occurrence of a massive data breach at Target stores. According to the report, Target was investigating the possible theft of millions of customer credit card and debit card records beginning November 27, 2013, and extending as far as December 15, 2013. The breach was thought to have occurred when thieves accessed the Company's customers' personal and financial data by breaking into Target's point-of-sale system.

**Target's Initial Reports of the Data Breach Provide False Assurances to Customers**

49. Consumers were entitled to adequate and prompt notification about the data breach to help them mitigate the harm and avoid additional instances of fraud. The Individual Defendants, however, failed to take reasonable steps to have the Company notify consumers that their information had been compromised. In so doing, the Individual Defendants aggravated the damage to affected customers.

50. Only after news of the data breach spread did the Company even mention the credit card attack. On December 19, 2013, over three weeks after the data breach

began, Target finally acknowledged the breach to the public. The Company issued a brief statement in which it confirmed that it had been aware of unauthorized access to certain customers' credit and debit card data at the Company's U.S. stores. According to the statement, "[a]pproximately **40 million** credit and debit card accounts may have been impacted between Nov. 27 and Dec. 15, 2013." In a separate statement issued that same day, Target conceded that customer data compromised in the data breach "included customer name, credit or debit card number, and the card's expiration date and CVV [card verification value]."

51. On December 20, 2013, in a rushed attempt to contain and minimize the perceived impact of the data breach, Target professed to "have worked swiftly to *resolve the incident*" and concluded that, "there is *no indication that PIN numbers have been compromised* on affected bank issued PIN debit cards or Target debit cards." Target assured worried customers that "[s]omeone cannot visit an ATM with a fraudulent debit card and withdraw cash." That same day, Target issued a press release announcing that "*the issue has been identified and eliminated*" and that the Company would provide free credit monitoring services to affected customers. In an effort to restore confidence in the Company, Target offered to extend its employees' discount of 10% to all customers who shopped in Target stores on December 21 and 22, 2013.

52. Despite Target's attempts to dispel customers' concerns, news began to emerge that credit and debit card information stolen from Target had begun to appear for sale online. According to an article by KrebsOnSecurity.com, customer account information stolen from Target was being sold on the black market "in batches of one

million cards" and fraudulent purchase activity had begun being reported by issuing banks.

53. As the growing scope of the breach continued to be revealed, Target confirmed on December 23, 2013, that the Secret Service and the DOJ decided to participate in the investigation into the breach. In addition, the Attorneys General from Massachusetts, New York, Connecticut, and South Dakota also began looking into the data breach.

54. The following day, *Reuters* reported that, despite prior statements by Target to the contrary, encrypted PIN data had been stolen during the original breach and that those codes could be used by thieves to make fraudulent withdrawals from the victims' bank accounts. In response to these allegations, Target continued to deny that any of its customers' PIN data had been compromised. As stated in defendant Steinhafel's letter to Target's customers published shortly after the Company's initial acknowledgment of the breach:

We want you to know a few important things:

- ☐ The unauthorized access took place in U.S. Target stores between Nov. 27 and Dec. 15, 2013. Canadian stores and target.com were not affected.
- ☐ *Even if you shopped at Target during this time frame, it doesn't mean you are a victim of fraud. In fact, in other similar situations, there are typically low levels of actual fraud.*
- ☐ There is *no indication that PIN numbers have been compromised* on affected bank issued PIN debit cards or Target debit cards. *Someone cannot visit an ATM with a fraudulent debit card and withdraw cash.*

- ☐ You will not be responsible for fraudulent charges—either your bank or Target have that responsibility.

### **The Full Scope of the Data Breach Is Revealed**

55. Then, on December 27, 2013, Target finally admitted that customers' PIN data had been compromised in the breach. Two weeks later, in yet another glaring indication that the Company had not yet "resolved" the matter, Target released a statement indicating that the breach was far more significant than the Company had been reporting. On January 10, 2014, Target disclosed that *70 million* customers may have been affected by the data breach, thirty million more victims that Target previously reported.

### **The Individual Defendants Knew or Should Have Known that the Company's Customers Were Vulnerable to Attack Yet Failed to Implement Appropriate Security Measures**

56. Target recognizes that its customers' personal and financial information is highly sensitive and must be protected. Moreover, as discussed above, Target promises its customers that it will "maintain administrative, technical and physical safeguards to protect [customers'] information" and "use industry standard methods to protect that information." Target's Privacy Policy states:

*We maintain administrative, technical and physical safeguards to protect your personal information. When we collect or transmit sensitive information such as a credit or debit card number, we use industry standard methods to protect that information.*

57. The PCI Data Security Standard ("PCI") is an industry standard for large retail institutions that accept credit card and debit card transactions. The standard consists of twelve general requirements including:

1. Install and maintain a firewall configuration to protect cardholder data;
  2. Do not use vendor-supplied defaults for system passwords and other security parameters;
  3. Protect stored cardholder data;
  4. Encrypt transmission of cardholder data across public networks;
  5. Use and regularly update anti-virus software or programs;
  6. Develop and maintain secure systems and applications;
  7. Restrict access to cardholder data by business need to know;
  8. Assign a unique ID to each person with computer access;
  9. Restrict physical access to cardholder data;
  10. Track and monitor all access to network resources and cardholder data;
  11. Regularly test security systems and processes; and
  12. Maintain a policy that addresses information security for all personnel.
58. On December 23, 2013, *USA Today* reported that Target was likely not

complying with the PCI. The article stated:

Target's massive databreach took place just a few weeks before a set of payment card industry standards – known as PCI DSS 3.0 – were scheduled to go into effect. CyberTruth asked Nick Aceto, technology director at software vendor CardConnect, to supply some clarity.

CyberTruth: What does this latest databreach tell us about the efficacy of PCI?

Aceto: We can't say definitely that this breach is a failure of Target's PCI compliance, but *based on what Target has said, it's very hard to believe that they were even PCI 2.0 compliant at the time of the breach.*

A reason for thinking this is that the attack, involving an enormous amount of data, went on essentially unnoticed for 18 days. How were they not watching the network?

One of the PCI DSS requirements is that you monitor your logs and firewalls every day, looking for unusual activity. This monitoring involves file integrity checks and changes to critical systems files. What's more – the chapter 6 software development life cycle requires the secure distribution and verification of payment applications.

Unusual activity isn't always abnormal, but the point of PCI is to monitor and verify that all activity is normal, while not letting distractions – like busy shopping days Black Friday and Cyber Monday, on which the breach occurred – detract from the monitoring effort.

59. The Individual Defendants knew or should have known that the Company's less than industry-standard security systems and unreasonably vulnerable technologies would render its customers an aim of attacks by third-parties. The Individual Defendants, however, failed to take corrective measures to update its systems and technologies. Among Target's deficiencies in this respect were its failure to maintain adequate backups and/or redundant systems; failure to encrypt data and establish adequate firewalls to handle a server intrusion contingency; and failure to provide prompt and adequate warnings of security breaches.

#### **DAMAGES TO TARGET**

60. As a result of the Individual Defendants' improprieties, thieves were able to steal sensitive personal and financial data from at least seventy million customers. Target's failure to protect its customers' personal and financial information has damaged its reputation with its customer base. In addition to price, Target's current and potential customers consider a company's ability to protect their personal and financial information

when choosing where to shop. Customers are less likely to shop at stores that cannot be trusted to safeguard their sensitive private information. The impact of the breach on the Company's bottom line has already begun to be revealed. In particular, the Company has experienced "meaningfully weaker-than-expected sales since the announcement," which lead the Company to cut its fourth quarter 2013 adjusted earnings per share ("EPS") of \$1.20 to \$1.30, compared to previous guidance of \$1.50 to \$1.60.

61. Further, as a direct and proximate result of the Individual Defendants' actions, Target has expended, and will continue to expend, significant sums of money. Such expenditures include, but are not limited to:

- (a) costs incurred from defending and paying any settlement in the numerous consumer class actions filed against the Company;

- (b) costs incurred from the Secret Service and DOJ investigations into the data breach, including, but not limited to, liability for any potential fines;

- (c) costs incurred from the Company's internal investigation into the data breach, including, but not limited to, expense for legal, investigative, and consulting fees;

- (d) costs incurred from expenses and capital investments for remediation activities;

- (e) costs incurred from notifying customers, replacing cards, sorting improper charges from legitimate charges, and reimbursing customers for improper charges;

(f) costs incurred from Target fulfilling its promise to provide free credit monitoring to victims of the data breach;

(g) loss of revenue and profit resulting from Target's offer of a 10% discount to U.S. shoppers during the last weekend before Christmas in an effort to lure customers back into its stores; and

(h) costs incurred from compensation and benefits paid to the defendants who have breached their duties to Target.

#### **DERIVATIVE AND DEMAND FUTILITY ALLEGATIONS**

62. Plaintiff brings this action derivatively in the right and for the benefit of Target to redress injuries suffered, and to be suffered, by Target as a direct result of breaches of fiduciary duty and waste of corporate assets, as well as the aiding and abetting thereof, by the Individual Defendants. Target is named as a nominal defendant solely in a derivative capacity. This is not a collusive action to confer jurisdiction on this Court that it would not otherwise have.

63. Plaintiff will adequately and fairly represent the interests of Target in enforcing and prosecuting its rights.

64. Plaintiff was a shareholder of Target at the time of the wrongdoing complained of, has continuously been a shareholder since that time, and is a current Target shareholder.

65. The current Board of Target consists of the following twelve individuals: defendants Austin, Baker, Darden, De Castro, Johnson, Minnick, Mulcahy, Rice, Salazar, Steinhafel, Stumpf, and Trujillo. Plaintiff has not made any demand on the present Board



to institute this action because such a demand would be a futile, wasteful, and useless act, as set forth below.

**Demand Is Excused Because the Director Defendants' Conduct Is Not a Valid Exercise of Business Judgment**

66. Defendants Austin, Baker, Darden, De Castro, Johnson, Minnick, Mulcahy, Rice, Salazar, Steinhafel, Stumpf, and Trujillo, constituting the Company's entire current Board, caused the Company to disseminate improper, materially false and misleading public statements concerning, among other things, the true nature and extent of the data breach. Consumers were entitled to adequate and prompt notification about the data breach to help them mitigate the harm and avoid additional instances of fraud. The Individual Defendants, however, failed to take reasonable steps to have the Company notify consumers that their information had been compromised. The Company's public disclosures concerning the data breach were improper because: (i) they were untimely and only released after third-party organizations began spreading the news; (ii) they understated the scope of the affected victims by thirty million people; and (iii) they diminished the severity of the harm to customers by failing to disclose that PINs were compromised. Each member of the Board knew or should have known that the improper statements did not timely, fairly, accurately, or truthfully convey the scope of the data breach. In addition, when deciding whether to approve statements to be publicly disseminated, each member of the Board was bound by the duty of care to inform himself or herself of all reasonably-available material information. Information concerning the nature and extent of the data breach was both reasonably available and material to

members of the Board. Defendants Austin, Baker, Darden, De Castro, Johnson, Minnick, Mulcahy, Rice, Salazar, Steinhafel, Stumpf, and Trujillo's conduct can in no way be considered a valid exercise of business judgment. Accordingly, demand on the Board is excused.

**Demand Is Excused Because the Entire Board Faces a Substantial Likelihood of Liability for Their Misconduct**

67. Defendants Austin, Baker, Darden, De Castro, Johnson, Minnick, Mulcahy, Rice, Salazar, Steinhafel, Stumpf, and Trujillo, all twelve members of the current Board, are disqualified from fairly evaluating the derivative claims, let alone vigorously prosecuting them, because they are each responsible for damages suffered by Target as a result of the Company's massive data breach. The Board was responsible for ensuring that internal controls were implemented and maintained to protect the Company's customers' personal and financial information. Instead, the Board failed to implement any internal controls to detect or prevent such a data breach from occurring. Despite each Individual Defendant's responsibility for "maintain[ing] administrative, technical, and physical safeguards to protect [customers'] personal information," defendants Austin, Baker, Darden, De Castro, Johnson, Minnick, Mulcahy, Rice, Salazar, Steinhafel, Stumpf, and Trujillo took no action to ensure such protection. These defendants' complete and utter failure to establish a system of appropriate internal controls and compliance measures is a breach of their duty of loyalty. As such, the entire Board faces a substantial likelihood of liability, rendering demand upon them futile.

68. Further, defendants Austin, Baker, Darden, De Castro, Johnson, Minnick, Mulcahy, Rice, Salazar, Steinhafel, Stumpf, and Trujillo face a substantial likelihood of liability due to their failure to provide adequate and prompt notice to consumers and because they conveyed a false sense of security to customers affected by the data breach. Defendants Austin, Baker, Darden, De Castro, Johnson, Minnick, Mulcahy, Rice, Salazar, Steinhafel, Stumpf, and Trujillo breached their duty of loyalty by causing the Company to disseminate the improper public statements discussed herein. Accordingly, all the Board members face a substantial likelihood of liability, further rendering demand upon them futile.

69. Any suit by the current directors of Target to remedy these wrongs would expose Target to liability in the numerous pending consumer class actions lawsuits. There are currently no less than nine consumer class actions filed against the Company as a result of the data breach. These class actions allege various claims, including, but not limited to, negligence, breach of contract, and violation of state privacy laws. If the Board elects for the Company to press forward with its right of action against any of the members of the Board in this action, then Target's efforts would compromise its defense of the pending consumer class actions. Accordingly, demand on the Board is excused.

70. The acts complained of constitute violations of the fiduciary duties owed by Target's officers and directors and these acts are incapable of ratification.

71. Target has been and will continue to be exposed to significant losses due to the wrongdoing complained of herein, yet the Individual Defendants and current Board have not filed any lawsuits against themselves or others who were responsible for that

wrongful conduct to attempt to recover for Target any part of the damages Target suffered and will suffer thereby.

72. Plaintiff has not made any demand on the other shareholders of Target to institute this action since such demand would be a futile and useless act for at least the following reasons:

(a) Target is a publicly held company with over 632 million shares outstanding and thousands of shareholders;

(b) making demand on such a number of shareholders would be impossible for plaintiff who has no way of finding out the names, addresses, or phone numbers of shareholders; and

(c) making demand on all shareholders would force plaintiff to incur excessive expenses, assuming all shareholders could be individually identified.

## **COUNT I**

### **Against the Individual Defendants for Breach of Fiduciary Duty**

73. Plaintiff incorporates by reference and realleges each and every allegation contained above, as though fully set forth herein.

74. As alleged in detail herein, the Individual Defendants, by reason of their positions as officers and directors of Target and because of their ability to control the business and corporate affairs of Target, owed to Target fiduciary obligations of due care and loyalty, and were and are required to use their utmost ability to control and manage Target in a fair, just, honest, and equitable manner.

75. The Officer Defendants breached their duty of loyalty by knowingly, recklessly, or with gross negligence: (i) failing to implement a system of internal controls to protect customers' personal and financial information; and (ii) causing or allowing the Company to conceal the full scope of the data breach, which affected at least seventy million customers.

76. The Director Defendants breached their duty of loyalty by knowingly or recklessly: (i) failing to implement a system of internal controls to protect customers' personal and financial information; and (ii) causing or allowing the Company to conceal the full scope of the data breach, which affected at least seventy million customers.

77. As a direct and proximate result of the Individual Defendants' breaches of their fiduciary obligations, Target has sustained significant damages, as alleged herein. As a result of the misconduct alleged herein, these defendants are liable to the Company.

78. Plaintiff, on behalf of Target, has no adequate remedy at law.

## **COUNT II**

### **Against all Individual Defendants for Waste of Corporate Assets**

79. Plaintiff incorporates by reference and realleges each and every allegation set forth above, as though fully set forth herein.

80. The wrongful conduct alleged included the failure to implement adequate internal controls to detect and prevent the breach of the Company's customers' personal and financial information. Under the Individual Defendants' purview, Target's customers became the victims of the second biggest data breach in retail history. The Company already incurred substantial costs in investigating the data breach and cooperating with

various government investigations. In addition, the Company lost revenue and profit due to its offer of a 10% discount to U.S. shoppers during the last weekend before Christmas in an effort to lure customers back into its stores after the data breach. The Company will continue to incur substantial costs from the numerous consumer class actions filed against it.

81. Further, the Individual Defendants caused Target to waste its assets by paying improper compensation and bonuses to certain of its executive officers and directors that breached their fiduciary duty.

82. As a result of the waste of corporate assets, the Individual Defendants are liable to the Company.

83. Plaintiff, on behalf of Target, has no adequate remedy at law.

#### **PRAYER FOR RELIEF**

WHEREFORE, plaintiff, on behalf of Target, demands judgment as follows:

A. Against the Individual Defendants and in favor of the Company for the amount of damages sustained by the Company as a result of the Individual Defendants' breach of fiduciary duty, waste of corporate assets, and aiding and abetting breaches of fiduciary duties;

B. Directing Target to take all necessary actions to reform and improve its corporate governance and internal procedures to comply with applicable laws and to protect the Company and its shareholders from a repeat of the damaging events described herein, including, but not limited to, putting forward for shareholder vote, resolutions for amendments to the Company's By-Laws or Articles of Incorporation, and taking such

other action as may be necessary to place before shareholders for a vote of the following Corporate Governance Policies:

1. a proposal to strengthen the Company's controls over its customers' personal and financial information;

2. a proposal to create a committee tasked with monitoring the Company's security measures;

3. a proposal to strengthen the Company's disclosure controls;

4. a proposal to strengthen the Board's supervision of operations and develop and implement procedures for greater shareholder input into the policies and guidelines of the Board; and

5. a provision to permit the shareholders of Target to nominate at least three candidates for election to the Board;

C. Awarding to Target restitution from the Individual Defendants, and each of them, and ordering disgorgement of all profits, benefits, and other compensation obtained by the Individual Defendants;

D. Awarding plaintiff the costs and disbursements of this action, including reasonable attorneys' and experts' fees, costs and expenses; and

E. Granting such other and further equitable relief as this Court may deem just and proper.

**JURY DEMAND**

Plaintiff demands a trial by jury.

Dated: January 21, 2014

**WALSH LAW FIRM**

*/s/Christopher R. Walsh*

**CHRISTOPHER R. WALSH (#199813)**

Attorney at Law

Fifth Street Towers

100 South Fifth Street, Suite 1025

Minneapolis, MN 55402

Telephone: 612-767-7500

Facsimile: 612-677-9300

walshlawfirm@comcast.net

**ROBBINS ARROYO LLP**

**BRIAN J. ROBBINS**

**FELIPE J. ARROYO**

**SHANE P. SANDERS**

600 B Street, Suite 1900

San Diego, CA 92101

Telephone: (619) 525-3990

Facsimile: (619) 525-3991

brobbins@robbinsarroyo.com

farroyo@robbinsarroyo.com

ssanders@robbinsarroyo.

Attorneys for Plaintiff



ROBERT KULLA

**UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF MINNESOTA**

MARY DAVIS, Derivatively on Behalf  
of TARGET CORPORATION,

Plaintiff,

v.

GREGG W. STEINHAFEL, BETH M.  
JACOB, JAMES A. JOHNSON,  
SOLOMON D. TRUJILLO, ANNE M.  
MULCAHY, ROXANNE S. AUSTIN,  
CALVIN DARDEN, MARY E.  
MINNICK, DERICA W. RICE, JOHN  
G. STUMPF, DOUGLAS M. BAKER,  
JR., HENRIQUE DE CASTRO, and  
KENNETH L. SALAZAR,

Defendants,

-and-

TARGET CORPORATION, a  
Minnesota corporation,

Nominal Defendant.

Case No. \_\_\_\_\_

**VERIFIED SHAREHOLDER  
DERIVATIVE COMPLAINT FOR  
BREACH OF FIDUCIARY DUTY  
AND WASTE OF CORPORATE  
ASSETS**

**DEMAND FOR JURY TRIAL**

### NATURE OF THE ACTION

1. This is a verified shareholder derivative action by plaintiff on behalf of nominal defendant Target Corporation ("Target" or the "Company") against certain of its officers and members of its Board of Directors (the "Board"). This action seeks to remedy defendants' violations of law, breaches of fiduciary duties, and waste of corporate assets that have caused substantial damages to the Company.

2. Target is the second largest general merchandise retailer in the United States. As part of its normal business practices, Target routinely collects its customers' personal and financial information, including credit and debit card numbers. Target assures its customers that it will protect this sensitive private information.

3. This action arises out of the Individual Defendants' (as defined herein) responsibility for the *second biggest data breach in retail history*. In violation of its express promise to do so, and contrary to reasonable customer expectations, Target failed to take reasonable steps to maintain its customers' personal and financial information in a secure manner. As a result of Target's complete and utter lack of appropriate security measures, thieves were able to steal sensitive personal and financial data from as many of *seventy million* customers who shopped at Target between November 27, 2013 and December 15, 2013, the height of the 2013 holiday season. For many of these victims, identity thieves have already utilized their personal information to commit fraud and other crimes. For tens of millions of others, constant vigilance of their financial and personal records will be required to protect themselves from the threat of having their identity stolen.

4. The Individual Defendants aggravated the damage to consumers from the data breach by failing to provide adequate and prompt notice to consumers and conveying a false sense of security to affected customers. In particular, the Individual Defendants allowed Target to delay acknowledging the breach to the public until December 19, 2013, over *three weeks* after the data breach began. Worse, Target disclosed the data breach only after third-party reports already broke the news. Even then, Target concealed the full nature and scope of the data breach. In particular, Target initially reported that the data breach affected forty million people and assured those affected by the data breach that "*the issue has been identified and eliminated*," and that there was "*no indication that [personal identification number ("PIN")] numbers have been compromised*." Target further reassured worried customers that "[s]omeone cannot visit an ATM with a fraudulent debit card and withdraw cash."

5. Despite these statements to the contrary, just days after Target's initial disclosure of the data breach, news outlets began reporting that encrypted PIN data had been stolen during the breach and that those codes could be used by thieves to make fraudulent withdrawals from the victims' bank accounts. In response to these allegations, Target continued to deny that any of its customers' PIN data had been compromised.

6. Then, on December 27, 2013, Target finally admitted that customers' PIN data had been compromised in the breach. Two weeks later, on January 10, 2014, Target released another statement indicating that the breach was far more significant than the Company had been reporting. In particular, Target disclosed that *seventy million*

customers may have been affected by the data breach, **30 million** more victims than Target previously reported.

7. The defendants' failures to implement any internal controls at Target designed to detect and prevent such a data breach, and then timely report it, have severely damaged Target. The Company's data breach is currently under investigation by the United States Secret Service ("Secret Service") and the Department of Justice ("DOJ"). Moreover, there are currently no less than **nine** class action lawsuits filed against Target on behalf of aggrieved customers. These class action lawsuits pose the risk of hundreds of millions of dollars in damages to the Company.

8. Plaintiff now brings this litigation on behalf of Target to rectify the conduct of the individuals bearing ultimate responsibility for the corporation's misconduct—the directors and senior management.

#### **JURISDICTION AND VENUE**

9. Jurisdiction is conferred by 28 U.S.C. §1332. Complete diversity among the parties exists and the amount in controversy exceeds \$75,000, exclusive of interest and costs.

10. This Court has jurisdiction over each defendant named herein because each defendant is either a corporation that conducts business in and maintains operations in this District, or is an individual who has sufficient minimum contacts with this District to render the exercise of jurisdiction by the District courts permissible under traditional notions of fair play and substantial justice.

11. Venue is proper in this Court in accordance with 28 U.S.C. §1391(a) because: (i) Target maintains its principal place of business in this District; (ii) one or more of the defendants either resides in or maintains executive offices in this District; (iii) a substantial portion of the transactions and wrongs complained of herein, including the defendants' primary participation in the wrongful acts detailed herein, and aiding and abetting and conspiracy in violation of fiduciary duties owed to Target, occurred in this District; and (iv) defendants have received substantial compensation in this District by doing business here and engaging in numerous activities that had an effect in this District.

#### **THE PARTIES**

##### **Plaintiff**

12. Plaintiff Mary Davis was a shareholder of Target at the time of the wrongdoing complained of, has continuously been a shareholder since that time, and is a current Target shareholder. Plaintiff is a citizen of New York.

##### **Nominal Defendant**

13. Nominal defendant Target is a Minnesota corporation with principal executive offices located at 1000 Nicollet Mall, Minneapolis, Minnesota. Accordingly, Target is a citizen of Minnesota. Target serves guests at 1,921 stores including 1,797 in the United States and 124 in Canada. The Company operates through three reportable segments: the U.S. Retail segment, which includes all of Target's U.S. merchandising operations; the U.S. Credit Card segment, which offers credit to qualified guests through its branded proprietary credit cards; and the Canadian segment which includes costs incurred in the U.S. and Canada related to the 2013 Canadian retail market entry.

**Defendants**

14. Defendant Gregg W. Steinhafel ("Steinhafel") is Target's Chief Executive Officer ("CEO") and has been since May 2008; President and has been since August 1999; Chairman of the Board and has been since February 2009; and a director and has been since 2007. Defendant Steinhafel has been employed by Target since 1979. Defendant Steinhafel knowingly, recklessly, or with gross negligence: (i) caused or allowed the Company to conceal the full scope of the data breach, which affected at least seventy million customers; and (ii) failed to implement a system of internal controls to protect customers' personal and financial information. Target paid defendant Steinhafel the following compensation as an executive:

Fiscal Year	Salary	Stock Awards	Option Awards	Non-Equity Incentive Plan Compensation	Change in Pension Value and Nonqualified Deferred Compensation	Other Compensation	Total
2012	\$1,500,000	\$5,285,245	\$5,248,573	\$2,880,000	\$665,528	\$5,068,118	\$20,647,464

Defendant Steinhafel is a citizen of Minnesota.

15. Defendant Beth M. Jacob ("Jacob") is Target's Chief Information Officer and has been since July 2008 and Executive Vice President, Target Technology Services and has been since January 2010. Defendant Jacob was also Senior Vice President, Target Technology Services from July 2008 to January 2010 and Vice President, Guest Operations, Target Financial Services from August 2006 to July 2008. Defendant Jacob knowingly, recklessly, or with gross negligence: (i) caused or allowed the Company to conceal the full scope of the data breach, which affected at least seventy million

customers; and (ii) failed to implement a system of internal controls to protect customers' personal and financial information. Defendant Jacob is a citizen of Minnesota.

16. Defendant James A. Johnson ("Johnson") is Target's Lead Independent Director and has been since at least April 2012 and a director and has been since 1996. Defendant Johnson is also a member of Target's Corporate Responsibility Committee and has been since at least April 2012. Defendant Johnson knowingly or recklessly: (i) caused or allowed the Company to conceal the full scope of the data breach, which affected at least seventy million customers; and (ii) failed to implement a system of internal controls to protect customers' personal and financial information. Target paid defendant Johnson the following compensation as a director:

<b>Fiscal Year</b>	<b>Fees Paid in Cash</b>	<b>Stock Awards</b>	<b>Option Awards</b>	<b>Change in Pension Value and Nonqualified Deferred Compensation</b>	<b>Total</b>
2012	\$135,000	\$90,055	\$71,477	\$13,174	\$309,706

Defendant Johnson is a citizen of Washington, D.C.

17. Defendant Solomon D. Trujillo ("Trujillo") is a Target director and has been since 1994. Defendant Trujillo is also Chairman of Target's Corporate Responsibility Committee and has been since at least April 2012. Defendant Trujillo knowingly or recklessly: (i) caused or allowed the Company to conceal the full scope of the data breach, which affected at least seventy million customers; and (ii) failed to implement a system of internal controls to protect customers' personal and financial information. Target paid defendant Trujillo the following compensation as a director:



<b>Fiscal Year</b>	<b>Fees Paid in Cash</b>	<b>Stock Awards</b>	<b>Option Awards</b>	<b>Change in Pension Value and Nonqualified Deferred Compensation</b>	<b>Total</b>
2012	\$105,000	\$90,055	\$71,477	\$32,165	\$298,697

Defendant Trujillo is a citizen of California.

18. Defendant Anne M. Mulcahy ("Mulcahy") is a Target director and has been since 1997. Defendant Mulcahy is also a member of Target's Audit Committee and has been since at least January 2014. Defendant Mulcahy knowingly or recklessly: (i) caused or allowed the Company to conceal the full scope of the data breach, which affected at least seventy million customers; and (ii) failed to implement a system of internal controls to protect customers' personal and financial information. Target paid defendant Mulcahy the following compensation as a director:

<b>Fiscal Year</b>	<b>Stock Awards</b>	<b>Total</b>
2012	\$275,003	\$275,003

Defendant Mulcahy is a citizen of Connecticut.

19. Defendant Roxanne S. Austin ("Austin") is a Target director and has been since 2002. Defendant Austin is also Chairman of Target's Audit Committee and has been since at least April 2012. Defendant Austin knowingly or recklessly: (i) caused or allowed the Company to conceal the full scope of the data breach, which affected at least seventy million customers; and (ii) failed to implement a system of internal controls to protect customers' personal and financial information. Target paid defendant Austin the following compensation as a director:

<b>Fiscal Year</b>	<b>Fees Paid in Cash</b>	<b>Stock Awards</b>	<b>Option Awards</b>	<b>Total</b>
2012	\$120,000	\$90,055	\$71,477	\$281,532

Defendant Austin is a citizen of California.

20. Defendant Calvin Darden ("Darden") is a Target director and has been since 2003. Defendant Darden is also a member of Target's Corporate Responsibility Committee and has been since at least January 2014. Defendant Darden knowingly or recklessly: (i) caused or allowed the Company to conceal the full scope of the data breach, which affected at least seventy million customers; and (ii) failed to implement a system of internal controls to protect customers' personal and financial information. Target paid defendant Darden the following compensation as a director:

<b>Fiscal Year</b>	<b>Fees Paid in Cash</b>	<b>Stock Awards</b>	<b>Option Awards</b>	<b>Total</b>
2012	\$90,000	\$90,055	\$71,477	\$251,532

Defendant Darden is a citizen of Georgia.

21. Defendant Mary E. Minnick ("Minnick") is a Target director and has been since 2005. Defendant Minnick is also a member of Target's Audit Committee and Corporate Responsibility Committee and has been since at least April 2012. Defendant Minnick knowingly or recklessly: (i) caused or allowed the Company to conceal the full scope of the data breach, which affected at least seventy million customers; and (ii) failed to implement a system of internal controls to protect customers' personal and financial information. Target paid defendant Minnick the following compensation as a director:

<b>Fiscal Year</b>	<b>Stock Awards</b>	<b>Total</b>
2012	\$260,004	\$260,004

Defendant Minnick is a citizen of the United Kingdom.

22. Defendant Derica W. Rice ("Rice") is a Target director and has been since 2007. Defendant Rice is also a member of Target's Audit Committee and has been since at least April 2012. Defendant Rice knowingly or recklessly: (i) caused or allowed the Company to conceal the full scope of the data breach, which affected at least seventy million customers; and (ii) failed to implement a system of internal controls to protect customers' personal and financial information. Target paid defendant Rice the following compensation as a director:

Fiscal Year	Stock Awards	Total
2012	\$260,004	\$260,004

Defendant Rice is a citizen of Indiana.

23. Defendant John G. Stumpf ("Stumpf") is a Target director and has been since 2010. Defendant Stumpf was also a member of Target's Audit Committee from at least April 2012 to March 2013. Defendant Stumpf knowingly or recklessly: (i) caused or allowed the Company to conceal the full scope of the data breach, which affected at least seventy million customers; and (ii) failed to implement a system of internal controls to protect customers' personal and financial information. Target paid defendant Stumpf the following compensation as a director:

Fiscal Year	Fees Paid in Cash	Stock Awards	Option Awards	Total
2012	\$90,000	\$90,055	\$71,477	\$251,532

Defendant Stumpf is a citizen of California.

24. Defendant Douglas M. Baker, Jr. ("Baker") is a Target director and has been since March 2013. Defendant Baker was also a member of Target's Audit

CASE 0:14-cv-00261-PAM-JJK Document 1 Filed 01/28/14 Page 11 of 35

Committee from March 2013 to at least April 2013. Defendant Baker knowingly or recklessly: (i) caused or allowed the Company to conceal the full scope of the data breach, which affected at least seventy million customers; and (ii) failed to implement a system of internal controls to protect customers' personal and financial information. Defendant Baker is a citizen of Minnesota.

25. Defendant Henrique De Castro ("De Castro") is a Target director and has been since March 2013. Defendant De Castro is also a member of Target's Corporate Responsibility Committee and has been since March 2013. Defendant De Castro knowingly or recklessly: (i) caused or allowed the Company to conceal the full scope of the data breach, which affected at least seventy million customers; and (ii) failed to implement a system of internal controls to protect customers' personal and financial information. Defendant De Castro is a citizen of California.

26. Defendant Kenneth L. Salazar ("Salazar") is a Target director and has been since July 2013. Defendant Salazar is also a member of Target's Corporate Responsibility Committee and has been since November 2013. Defendant Salazar knowingly or recklessly: (i) caused or allowed the Company to conceal the full scope of the data breach, which affected at least seventy million customers; and (ii) failed to implement a system of internal controls to protect customers' personal and financial information. Defendant Salazar is a citizen of Colorado.

27. The defendants identified in ¶¶14-15 are referred to herein as the "Officer Defendants." The defendants identified in ¶¶16-26 are referred to herein as the "Director

Defendants." Collectively, the defendants identified in ¶¶14-26 are referred to herein as the "Individual Defendants."

### **DUTIES OF THE INDIVIDUAL DEFENDANTS**

#### **Fiduciary Duties**

28. By reason of their positions as officers and directors of the Company, each of the Individual Defendants owed and owe Target and its shareholders fiduciary obligations of trust, loyalty, good faith, and due care, and were and are required to use their utmost ability to control and manage Target in a fair, just, honest, and equitable manner. The Individual Defendants were and are required to act in furtherance of the best interests of Target and not in furtherance of their personal interest or benefit.

29. To discharge their duties, the officers and directors of Target were required to exercise reasonable and prudent supervision over the management, policies, practices, and controls of the financial affairs of the Company. By virtue of such duties, the officers and directors of Target were required to, among other things:

- (a) devise and maintain a system of internal controls sufficient to ensure that the Company's customers' personal and financial information is protected;
- (b) ensure that the Company timely and accurately informed customers regarding any breach of their personal and financial information;
- (c) conduct the affairs of the Company in an efficient, business-like manner in compliance with all applicable laws, rules, and regulations so as to make it possible to provide the highest quality performance of its business, to avoid wasting the Company's assets, and to maximize the value of the Company's stock; and

(d) remain informed as to how Target conducted its operations, and, upon receipt of notice or information of imprudent or unsound conditions or practices, make reasonable inquiry in connection therewith, and take steps to correct such conditions or practices.

#### **Breaches of Duties**

30. The conduct of the Individual Defendants complained of herein involves a knowing and culpable violation of their obligations as officers and directors of Target, the absence of good faith on their part, and a reckless disregard for their duties to the Company that the Individual Defendants were aware or reckless in not being aware posed a risk of serious injury to the Company.

31. The Individual Defendants, because of their positions of control and authority as officers and/or directors of Target, were able to and did, directly or indirectly, exercise control over the wrongful acts complained of herein. The Individual Defendants also failed to prevent the other Individual Defendants from taking such illegal actions. As a result, and in addition to the damage the Company has already incurred, Target has expended, and will continue to expend, significant sums of money.

#### **CONSPIRACY, AIDING AND ABETTING, AND CONCERTED ACTION**

32. In committing the wrongful acts alleged herein, the Individual Defendants have pursued, or joined in the pursuit of, a common course of conduct, and have acted in concert with and conspired with one another in furtherance of their common plan or design. In addition to the wrongful conduct herein alleged as giving rise to primary

liability, the Individual Defendants further aided and abetted and/or assisted each other in breaching their respective duties.

33. The Individual Defendants engaged in a conspiracy, common enterprise, and/or common course of conduct. During this time, the Individual Defendants failed to timely and accurately inform customers regarding the full scope of the breach of their personal and financial information.

34. The purpose and effect of the Individual Defendants' conspiracy, common enterprise, and/or common course of conduct was, among other things, to disguise the Individual Defendants' violations of law, breaches of fiduciary duty, and waste of corporate assets; and to conceal adverse information concerning the Company's operations.

35. The Individual Defendants accomplished their conspiracy, common enterprise, and/or common course of conduct by allowing the Company to purposefully or recklessly conceal the scope of the data breach affecting at least seventy million customers. Because the actions described herein occurred under the authority of the Board, each of the Individual Defendants was a direct, necessary, and substantial participant in the conspiracy, common enterprise, and/or common course of conduct complained of herein.

36. Each of the Individual Defendants aided and abetted and rendered substantial assistance in the wrongs complained of herein. In taking such actions to substantially assist the commission of the wrongdoing complained of herein, each Individual Defendant acted with knowledge of the primary wrongdoing, substantially

CASE 0:14-cv-00261-PAM-JJK Document 1 Filed 01/28/14 Page 15 of 35

assisted in the accomplishment of that wrongdoing, and was aware of his or her overall contribution to and furtherance of the wrongdoing.

#### **BACKGROUND OF THE COMPANY AND ITS PRIVACY POLICY**

37. Target is the second largest general merchandise retailer in the United States. The Company operates 1,797 stores in the United States and 124 stores in Canada.

38. As stated in the Company's own "Privacy Policy," Target routinely collects personal information from its customers including a customer's name, mailing address, e-mail address, phone number, driver's license number, and credit/debit card number. In addition, when customers use their debit cards to make a purchase at Target, they are required to enter the PIN associated with their bank account. Target promises its customers that it will, among other things, "*maintain administrative, technical and physical safeguards to protect your personal information*." When we collect or transmit sensitive information such as a credit or debit card number, *we use industry standard methods to protect that information*."

#### **The Ramifications of Failing to Keep Customers' Data Secure Are Severe**

39. Notwithstanding its promise and duties to protect its customers' sensitive personal and financial information, Target allowed the sensitive and private information of tens of millions of its customers to be stolen. Target's failure to protect its customers' sensitive personal and financial information exposes victims to identity theft. Identity theft occurs when someone wrongfully obtains another's personal information without their knowledge to commit theft or fraud.



40. Armed with a person's personal and financial information, identity thieves can encode the victim's account information onto a different card with a magnetic strip creating a counterfeit card that can be used to make fraudulent purchases. With the addition of a victim's PIN, a thief can use the counterfeit card to withdraw money from that person's bank account.

41. Identity thieves can cause further damage to their victims by using personal information to open new credit and utility accounts, receive medical treatment on their health insurance, or even obtain a driver's license. Once a person's identity has been stolen, reporting, identifying, monitoring, and repairing the victim's credit is a cumbersome, expensive, and time-consuming process. In addition to the frustration of having to identify and close affected accounts, correct information in their credit reports, victims of identity theft often incur costs associated with defending themselves against civil litigation brought by creditors. Victims also suffer the burden of having difficulty obtaining new credit. Moreover, victims of identity theft must monitor their credit reports for future inaccuracies as fraudulent use of stolen personal information may persist for several years.

42. Annual monetary losses from identity theft are in the billions of dollars. According to The President's Identity Theft Task Force Report dated October 21, 2008, on identity theft produced in 2008:

In addition to the losses that result when identity thieves fraudulently open accounts or misuse existing accounts, ... individual victims often suffer indirect financial costs, including the costs incurred in both civil litigation initiated by creditors and in overcoming the many obstacles they face in obtaining or retaining credit. Victims of non-financial identity theft, for

example, health-related or criminal record fraud, face other types of harm and frustration.

In addition to out-of-pocket expenses that can reach thousands of dollars for the victims of new account identity theft, and the emotional toll identity theft can take, some victims have to spend what can be a considerable amount of time to repair the damage caused by the identity thieves. Victims of new account identity theft, for example, must correct fraudulent information in their credit reports and monitor their reports for future inaccuracies, close existing bank accounts and open new ones, and dispute charges with individual creditors.

43. The significant impact identity theft can have on consumers and the extreme financial ramification the failure to secure personal information can cause has led to the enactment of numerous privacy-related laws aimed toward protecting consumer information and disclosure requirements, including, for example: (i) Gramm-Leach-Bliley Act; (ii) Fair Credit Reporting Act; (iii) Fair and Accurate Credit Transactions Act; (iv) Federal Trade Commission Act, 15 U.S.C. §§41-58; (v) Driver's Privacy Protection Act; (vi) Health Insurance Portability and Accountability Act; (vii) The Privacy Act of 1974; (viii) Social Security Act Amendments of 1990; (ix) E-Government Act of 2002; and (x) Federal Information Security Management Act of 2002.

44. Moreover, the recent wave of cyber-attacks striking American corporations prompted warnings from federal officials, including one issued in May 2013 by the Department of Homeland Security. In particular, the warning was issued by an agency called ICS-Cert, which monitors attacks on computer systems that run industrial processes. The warning stated that the government was "highly concerned about hostility against critical infrastructure organizations."

45. The Individual Defendants were fully aware of the risk of a potential data breach. On August 27, 2007, Dr. Neal Krawetz, a data security expert working for Hacker Factor Solutions, publicly disclosed a white paper<sup>1</sup> titled "Point-of-Sale Vulnerabilities" (the "White Paper") warning Target about the possibility of a point-of-sale data breach. The White Paper used Target as an example of the potential ramifications of a point-of-sale data breach at a major retailer and estimated that as many as fifty-eight million card accounts could be compromised if Target's point-of-sale system was compromised.

46. Moreover, the Individual Defendants were fully aware of the ramifications of failing to keep customers' data secure and knew that the Company could be subject to costly government enforcement actions and private litigation. As stated in the risk disclosures in the Company's Annual Report on Form 10-K filed with the U.S. Securities and Exchange Commission ("SEC") on March 20, 2013:

*If we experience a significant data security breach or fail to detect and appropriately respond to a significant data security breach, we could be exposed to government enforcement actions and private litigation. In addition, our guests could lose confidence in our ability to protect their personal information, which could cause them to discontinue usage of REDcards, decline to use our pharmacy services, or stop shopping with us altogether. The loss of confidence from a significant data security breach involving team members could hurt our reputation, cause team member recruiting and retention challenges, increase our labor costs and affect how we operate our business.*

---

<sup>1</sup> A white paper is an authoritative report or guide helping readers to understand an issue, solve a problem, or make a decision. White papers are used in two main spheres: government and business-to-business marketing.

**THE INDIVIDUAL DEFENDANTS' FAILURE TO PROTECT CUSTOMERS' PERSONAL INFORMATION LEADS TO RECORD-SETTING DATA BREACH**

47. Target's data breach compromised seventy million customers' personal and financial data. Within days of the breach, millions of affected customers' financial and personal information was being sold on the black-market. Moreover, bank cards that had only been used at Target were found to have been used to make unauthorized purchases at Target stores.

48. News of the data breach first broke out on December 18, 2013, when KrebsOnSecurity.com, a website dedicated to reporting cybercrime, published an article indicating the occurrence of a massive data breach at Target stores. According to the report, Target was investigating the possible theft of millions of customer credit card and debit card records beginning November 27, 2013, and extending as far as December 15, 2013. The breach was thought to have occurred when thieves accessed the Company's customers' personal and financial data by breaking into Target's point-of-sale system.

**Target's Initial Reports of the Data Breach Provide False Assurances to Customers**

49. Consumers were entitled to adequate and prompt notification about the data breach to help them mitigate the harm and avoid additional instances of fraud. The Individual Defendants, however, failed to take reasonable steps to have the Company notify consumers that their information had been compromised. In so doing, the Individual Defendants aggravated the damage to affected customers.

50. Only after news of the data breach spread did the Company even mention the credit card attack. On December 19, 2013, over three weeks after the data breach

began, Target finally acknowledged the breach to the public. The Company issued a brief statement in which it confirmed that it had been aware of unauthorized access to certain customers' credit and debit card data at the Company's U.S. stores. According to the statement, "[a]pproximately **40 million** credit and debit card accounts may have been impacted between Nov. 27 and Dec. 15, 2013." In a separate statement issued that same day, Target conceded that customer data compromised in the data breach "included customer name, credit or debit card number, and the card's expiration date and CVV [card verification value]."

51. On December 20, 2013, in a rushed attempt to contain and minimize the perceived impact of the data breach, Target professed to "have worked swiftly to *resolve the incident*" and concluded that, "there is *no indication that PIN numbers have been compromised* on affected bank issued PIN debit cards or Target debit cards." Target assured worried customers that "[s]omeone cannot visit an ATM with a fraudulent debit card and withdraw cash." That same day, Target issued a press release announcing that "*the issue has been identified and eliminated*" and that the Company would provide free credit monitoring services to affected customers. In an effort to restore confidence in the Company, Target offered to extend its employees' discount of 10% to all customers who shopped in Target stores on December 21 and 22, 2013.

52. Despite Target's attempts to dispel customers' concerns, news began to emerge that credit and debit card information stolen from Target had begun to appear for sale online. According to an article by KrebsOnSecurity.com, customer account information stolen from Target was being sold on the black market "in batches of one

million cards" and fraudulent purchase activity had begun being reported by issuing banks.

53. As the growing scope of the breach continued to be revealed, Target confirmed on December 23, 2013, that the Secret Service and the DOJ decided to participate in the investigation into the breach. In addition, the Attorneys General from Massachusetts, New York, Connecticut, and South Dakota also began looking into the data breach.

54. The following day, *Reuters* reported that, despite prior statements by Target to the contrary, encrypted PIN data had been stolen during the original breach and that those codes could be used by thieves to make fraudulent withdrawals from the victims' bank accounts. In response to these allegations, Target continued to deny that any of its customers' PIN data had been compromised. As stated in defendant Steinhafel's letter to Target's customers published shortly after the Company's initial acknowledgment of the breach:

We want you to know a few important things:

- The unauthorized access took place in U.S. Target stores between Nov. 27 and Dec. 15, 2013. Canadian stores and target.com were not affected.
- *Even if you shopped at Target during this time frame, it doesn't mean you are a victim of fraud. In fact, in other similar situations, there are typically low levels of actual fraud.*
- There is *no indication that PIN numbers have been compromised* on affected bank issued PIN debit cards or Target debit cards. *Someone cannot visit an ATM with a fraudulent debit card and withdraw cash.*

- You will not be responsible for fraudulent charges—either your bank or Target have that responsibility.

### **The Full Scope of the Data Breach Is Revealed**

55. Then, on December 27, 2013, Target finally admitted that customers' PIN data had been compromised in the breach. Two weeks later, in yet another glaring indication that the Company had not yet "resolved" the matter, Target released a statement indicating that the breach was far more significant than the Company had been reporting. On January 10, 2014, Target disclosed that *70 million* customers may have been affected by the data breach, thirty million more victims that Target previously reported.

### **The Individual Defendants Knew or Should Have Known that the Company's Customers Were Vulnerable to Attack yet Failed to Implement Appropriate Security Measures**

56. Target is aware and has stated that its customers' personal and financial information is highly sensitive and must be protected. Moreover, as discussed above, Target promises its customers that it will "maintain administrative, technical and physical safeguards to protect [customers'] information" and "use industry standard methods to protect that information." Target's Privacy Policy states:

*We maintain administrative, technical and physical safeguards to protect your personal information.* When we collect or transmit sensitive information such as a credit or debit card number, *we use industry standard methods* to protect that information.

57. The PCI Data Security Standard ("PCI") is an industry standard for large retail institutions that accept credit card and debit card transactions. The standard consists of twelve general requirements including:

CASE 0:14-cv-00261-PAM-JJK Document 1 Filed 01/28/14 Page 23 of 35

1. Install and maintain a firewall configuration to protect cardholder data;
  2. Do not use vendor-supplied defaults for system passwords and other security parameters;
  3. Protect stored cardholder data;
  4. Encrypt transmission of cardholder data across public networks;
  5. Use and regularly update anti-virus software or programs;
  6. Develop and maintain secure systems and applications;
  7. Restrict access to cardholder data by business need to know;
  8. Assign a unique ID to each person with computer access;
  9. Restrict physical access to cardholder data;
  10. Track and monitor all access to network resources and cardholder data;
  11. Regularly test security systems and processes; and
  12. Maintain a policy that addresses information security for all personnel.
58. On December 23, 2013, *USA Today* reported that Target was likely not

complying with the PCI. The article stated:

Target's massive databreach took place just a few weeks before a set of payment card industry standards – known as PCI DSS 3.0 – were scheduled to go into effect. CyberTruth asked Nick Aceto, technology director at software vendor CardConnect, to supply some clarity.

CyberTruth: What does this latest databreach tell us about the efficacy of PCI?

Aceto: We can't say definitely that this breach is a failure of Target's PCI compliance, but *based on what Target has said, it's very hard to believe that they were even PCI 2.0 compliant at the time of the breach.*



CASE 0:14-cv-00261-PAM-JJK Document 1 Filed 01/28/14 Page 24 of 35

A reason for thinking this is that the attack, involving an enormous amount of data, went on essentially unnoticed for 18 days. How were they not watching the network?

One of the PCI DSS requirements is that you monitor your logs and firewalls every day, looking for unusual activity. This monitoring involves file integrity checks and changes to critical systems files. What's more – the chapter 6 software development life cycle requires the secure distribution and verification of payment applications.

Unusual activity isn't always abnormal, but the point of PCI is to monitor and verify that all activity is normal, while not letting distractions – like busy shopping days Black Friday and Cyber Monday, on which the breach occurred – detract from the monitoring effort.

59. The Individual Defendants knew or should have known that the Company's less than industry-standard security systems and unreasonably vulnerable technologies would render its customers an aim of attacks by third-parties. The Individual Defendants, however, failed to take corrective measures to update its systems and technologies. Among Target's deficiencies in this respect were its failure to maintain adequate backups and/or redundant systems; failure to encrypt data and establish adequate firewalls to handle a server intrusion contingency; and failure to provide prompt and adequate warnings of security breaches.

#### **DAMAGES TO TARGET**

60. As a result of the Individual Defendants' improprieties, thieves were able to steal sensitive personal and financial data from at least seventy million customers. Target's failure to protect its customers' personal and financial information has damaged its reputation with its customer base. In addition to price, Target's current and potential customers consider a company's ability to protect their personal and financial information

when choosing where to shop. Customers are less likely to shop at stores that cannot be trusted to safeguard their sensitive private information. The impact of the breach on the Company's bottom line has already begun to be revealed. In particular, the Company has experienced "meaningfully weaker-than-expected sales since the announcement," which lead the Company to cut its fourth quarter 2013 adjusted earnings per share ("EPS") of \$1.20 to \$1.30, compared to previous guidance of \$1.50 to \$1.60.

61. Further, as a direct and proximate result of the Individual Defendants' actions, Target has expended, and will continue to expend, significant sums of money. Such expenditures include, but are not limited to:

- (a) costs incurred from defending and paying any settlement in the numerous consumer class actions filed against the Company;

- (b) costs incurred from the Secret Service and DOJ investigations into the data breach, including, but not limited to, liability for any potential fines;

- (c) costs incurred from the Company's internal investigation into the data breach, including, but not limited to, expense for legal, investigative, and consulting fees;

- (d) costs incurred from expenses and capital investments for remediation activities;

- (e) costs incurred from notifying customers, replacing cards, sorting improper charges from legitimate charges, and reimbursing customers for improper charges;

(f) costs incurred from Target fulfilling its promise to provide free credit monitoring to victims of the data breach;

(g) loss of revenue and profit resulting from Target's offer of a 10% discount to U.S. shoppers during the last weekend before Christmas in an effort to lure customers back into its stores; and

(h) costs incurred from compensation and benefits paid to the defendants who have breached their duties to Target.

#### **DERIVATIVE AND DEMAND FUTILITY ALLEGATIONS**

62. Plaintiff brings this action derivatively in the right and for the benefit of Target to redress injuries suffered, and to be suffered, by Target as a direct result of breaches of fiduciary duty and waste of corporate assets, as well as the aiding and abetting thereof, by the Individual Defendants. Target is named as a nominal defendant solely in a derivative capacity. This is not a collusive action to confer jurisdiction on this Court that it would not otherwise have.

63. Plaintiff will adequately and fairly represent the interests of Target in enforcing and prosecuting its rights.

64. Plaintiff was a shareholder of Target at the time of the wrongdoing complained of, has continuously been a shareholder since that time, and is a current Target shareholder.

65. The current Board of Target consists of the following twelve individuals: defendants Austin, Baker, Darden, De Castro, Johnson, Minnick, Mulcahy, Rice, Salazar, Steinhafel, Stumpf, and Trujillo. Plaintiff has not made any demand on the present Board

to institute this action because such a demand would be a futile, wasteful, and useless act, as set forth below.

**Demand Is Excused Because the Director Defendants' Conduct Is Not a Valid Exercise of Business Judgment**

66. Defendants Austin, Baker, Darden, De Castro, Johnson, Minnick, Mulcahy, Rice, Salazar, Steinhafel, Stumpf, and Trujillo, constituting the Company's entire current Board, caused the Company to disseminate improper, materially false and misleading public statements concerning, among other things, the true nature and extent of the data breach. Consumers were entitled to adequate and prompt notification about the data breach to help them mitigate the harm and avoid additional instances of fraud. The Individual Defendants, however, failed to take reasonable steps to have the Company notify consumers that their information had been compromised. The Company's public disclosures concerning the data breach were improper because: (i) they were untimely and only released after third-party organizations began spreading the news; (ii) they understated the scope of the affected victims by thirty million people; and (iii) they diminished the severity of the harm to customers by failing to disclose that PINs were compromised. Each member of the Board knew or should have known that the improper statements did not timely, fairly, accurately, or truthfully convey the scope of the data breach. In addition, when deciding whether to approve statements to be publicly disseminated, each member of the Board was bound by the duty of care to inform himself or herself of all reasonably-available material information. Information concerning the nature and extent of the data breach was both reasonably available and material to

members of the Board. Defendants Austin, Baker, Darden, De Castro, Johnson, Minnick, Mulcahy, Rice, Salazar, Steinhafel, Stumpf, and Trujillo's conduct can in no way be considered a valid exercise of business judgment. Accordingly, demand on the Board is excused.

**Demand Is Excused Because the Entire Board Faces a Substantial Likelihood of Liability for Their Misconduct**

67. Defendants Austin, Baker, Darden, De Castro, Johnson, Minnick, Mulcahy, Rice, Salazar, Steinhafel, Stumpf, and Trujillo, all twelve members of the current Board, are disqualified from fairly evaluating the derivative claims, let alone vigorously prosecuting them, because they are each responsible for damages suffered by Target as a result of the Company's massive data breach. The Board was responsible for ensuring that internal controls were implemented and maintained to protect the Company's customers' personal and financial information. Instead, the Board failed to implement any internal controls to detect or prevent such a data breach from occurring. Despite each Individual Defendant's responsibility for "maintain[ing] administrative, technical, and physical safeguards to protect [customers'] personal information," defendants Austin, Baker, Darden, De Castro, Johnson, Minnick, Mulcahy, Rice, Salazar, Steinhafel, Stumpf, and Trujillo took no action to ensure such protection. These defendants' complete and utter failure to establish a system of appropriate internal controls and compliance measures is a breach of their duty of loyalty. As such, the entire Board faces a substantial likelihood of liability, rendering demand upon them futile.

68. Further, defendants Austin, Baker, Darden, De Castro, Johnson, Minnick, Mulcahy, Rice, Salazar, Steinhafel, Stumpf, and Trujillo face a substantial likelihood of liability due to their failure to provide adequate and prompt notice to consumers and because they conveyed a false sense of security to customers affected by the data breach. Defendants Austin, Baker, Darden, De Castro, Johnson, Minnick, Mulcahy, Rice, Salazar, Steinhafel, Stumpf, and Trujillo breached their duty of loyalty by causing the Company to disseminate the improper public statements discussed herein. Accordingly, all the Board members face a substantial likelihood of liability, further rendering demand upon them futile.

69. Any suit by the current directors of Target to remedy these wrongs would expose Target to liability in the numerous pending consumer class actions lawsuits. There are currently no less than nine consumer class actions filed against the Company as a result of the data breach. These class actions allege various claims, including, but not limited to, negligence, breach of contract, and violation of state privacy laws. If the Board elects for the Company to press forward with its right of action against any of the members of the Board in this action, then Target's efforts would compromise its defense of the pending consumer class actions. Accordingly, demand on the Board is excused.

70. The acts complained of constitute violations of the fiduciary duties owed by Target's officers and directors and these acts are incapable of ratification.

71. Target has been and will continue to be exposed to significant losses due to the wrongdoing complained of herein, yet the Individual Defendants and current Board have not filed any lawsuits against themselves or others who were responsible for that

CASE 0:14-cv-00261-PAM-JJK Document 1 Filed 01/28/14 Page 30 of 35

wrongful conduct to attempt to recover for Target any part of the damages Target suffered and will suffer thereby.

72. Plaintiff has not made any demand on the other shareholders of Target to institute this action since such demand would be a futile and useless act for at least the following reasons:

(a) Target is a publicly held company with over 632 million shares outstanding and thousands of shareholders;

(b) making demand on such a number of shareholders would be impossible for plaintiff who has no way of finding out the names, addresses, or phone numbers of shareholders; and

(c) making demand on all shareholders would force plaintiff to incur excessive expenses, assuming all shareholders could be individually identified.

#### **COUNT I**

##### **Against the Individual Defendants for Breach of Fiduciary Duty**

73. Plaintiff incorporates by reference and realleges each and every allegation contained above, as though fully set forth herein.

74. As alleged in detail herein, the Individual Defendants, by reason of their positions as officers and directors of Target and because of their ability to control the business and corporate affairs of Target, owed to Target fiduciary obligations of due care and loyalty, and were and are required to use their utmost ability to control and manage Target in a fair, just, honest, and equitable manner.

75. The Officer Defendants breached their duty of loyalty by knowingly, recklessly, or with gross negligence: (i) failing to implement a system of internal controls to protect customers' personal and financial information; and (ii) causing or allowing the Company to conceal the full scope of the data breach, which affected at least seventy million customers.

76. The Director Defendants breached their duty of loyalty by knowingly or recklessly: (i) failing to implement a system of internal controls to protect customers' personal and financial information; and (ii) causing or allowing the Company to conceal the full scope of the data breach, which affected at least seventy million customers.

77. As a direct and proximate result of the Individual Defendants' breaches of their fiduciary obligations, Target has sustained significant damages, as alleged herein. As a result of the misconduct alleged herein, these defendants are liable to the Company.

78. Plaintiff, on behalf of Target, has no adequate remedy at law.

## **COUNT II**

### **Against all Individual Defendants for Waste of Corporate Assets**

79. Plaintiff incorporates by reference and realleges each and every allegation set forth above, as though fully set forth herein.

80. The wrongful conduct alleged included the failure to implement adequate internal controls to detect and prevent the breach of the Company's customers' personal and financial information. Under the Individual Defendants' purview, Target's customers became the victims of the second biggest data breach in retail history. The Company already incurred substantial costs in investigating the data breach and cooperating with



various government investigations. In addition, the Company lost revenue and profit due to its offer of a 10% discount to U.S. shoppers during the last weekend before Christmas in an effort to lure customers back into its stores after the data breach. The Company will continue to incur substantial costs from the numerous consumer class actions filed against it.

81. Further, the Individual Defendants caused Target to waste its assets by paying improper compensation and bonuses to certain of its executive officers and directors that breached their fiduciary duty.

82. As a result of the waste of corporate assets, the Individual Defendants are liable to the Company.

83. Plaintiff, on behalf of Target, has no adequate remedy at law.

#### **PRAYER FOR RELIEF**

WHEREFORE, plaintiff, on behalf of Target, demands judgment as follows:

A. Against the Individual Defendants and in favor of the Company for the amount of damages sustained by the Company as a result of the Individual Defendants' breach of fiduciary duty, waste of corporate assets, and aiding and abetting breaches of fiduciary duties;

B. Directing Target to take all necessary actions to reform and improve its corporate governance and internal procedures to comply with applicable laws and to protect the Company and its shareholders from a repeat of the damaging events described herein, including, but not limited to, putting forward for shareholder vote, resolutions for amendments to the Company's By-Laws or Articles of Incorporation, and taking such

CASE 0:14-cv-00261-PAM-JJK Document 1 Filed 01/28/14 Page 33 of 35

other action as may be necessary to place before shareholders for a vote of the following Corporate Governance Policies:

1. a proposal to strengthen the Company's controls over its customers' personal and financial information;
  2. a proposal to create a committee tasked with monitoring the Company's security measures;
  3. a proposal to strengthen the Company's disclosure controls;
  4. a proposal to strengthen the Board's supervision of operations and develop and implement procedures for greater shareholder input into the policies and guidelines of the Board; and
  5. a provision to permit the shareholders of Target to nominate at least three candidates for election to the Board;
- C. Awarding to Target restitution from the Individual Defendants, and each of them, and ordering disgorgement of all profits, benefits, and other compensation obtained by the Individual Defendants;
- D. Awarding plaintiff the costs and disbursements of this action, including reasonable attorneys' and experts' fees, costs and expenses; and
- E. Granting such other and further equitable relief as this Court may deem just and proper.

CASE 0:14-cv-00261-PAM-JJK Document 1 Filed 01/28/14 Page 34 of 35

**JURY DEMAND**

Plaintiff demands a trial by jury.

Dated: January 28, 2014

**WALSH LAW FIRM**

*/s/Christopher R. Walsh*

CHRISTOPHER R. WALSH (#199813)

Attorney at Law

Fifth Street Towers

100 South Fifth Street, Suite 1025

Minneapolis, MN 55402

Telephone: 612-767-7500

Facsimile: 612-677-9300

walshlawfirm@comcast.net

LAW OFFICE OF DEBRA S.

GOODMAN P.C.

DEBRA S. GOODMAN

1301 Skippack Pike, Suite 7A #133

Blue Bell, PA 19422

Telephone: (610) 277-6057

Facsimile: (484) 231-1922

debbie419@comcast.net

Attorneys for Plaintiff

VERIFICATION

I, Mary Davis, hereby declare as follows:

I am the plaintiff in the within entitled action. I have read the Verified Shareholder Derivative Complaint for Breach of Fiduciary Duty and Waste of Corporate Assets. Based upon discussions with and reliance upon my counsel, and as to those facts of which I have personal knowledge, the Complaint is true and correct to the best of my knowledge, information, and belief.

I declare under penalty of perjury that the foregoing is true and correct.

Signed and Accepted:

Dated: 1-27-14

Mary J. Davis  
MARY DAVIS

## CASE 0:14-cv-00261-PAM-JJK Document 1-1 Filed 01/28/14 Page 1 of 2

JS 44 (Rev. 12/12)

## CIVIL COVER SHEET

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. (SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)

## I. (a) PLAINTIFFS

MARY DAVIS, Derivatively on Behalf of TARGET CORPORATION

(b) County of Residence of First Listed Plaintiff New York, New York  
(EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys (Firm Name, Address, and Telephone Number)

Christopher R. Walsh (#199813), Walsh Law Firm, Fifth Street Towers,  
100 South Fifth Street, Suite 1025, Minneapolis, MN 55402; Telephone  
(612) 767-7500

## DEFENDANTS

GREGG W. STEINHAFEL, BETH M. JACOB, JAMES A. JOHNSON,  
SOLOMON D. TRUJILLO, ANNE M. MULCAHY, ROXANNE S.  
AUSTIN, CALVIN DARDEN, MARY E. MINNICK, et al.

County of Residence of First Listed Defendant Hennepin County, MN  
(IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF  
THE TRACT OF LAND INVOLVED.

Attorneys (If Known)

## II. BASIS OF JURISDICTION (Place an "X" in One Box Only)

- ☐ 1 U.S. Government Plaintiff  
☐ 2 U.S. Government Defendant  
☐ 3 Federal Question (U.S. Government Not a Party)  
☒ 4 Diversity (Indicate Citizenship of Parties in Item III)

## III. CITIZENSHIP OF PRINCIPAL PARTIES (Place an "X" in One Box for Plaintiff and One Box for Defendant)

- |   | PTF                                   | DEF                        |   | PTF                        | DEF                                   |
|---|---------------------------------------|----------------------------|---|----------------------------|---------------------------------------|
| Citizen of This State                   | <input type="checkbox"/> 1            | <input type="checkbox"/> 1 | Incorporated or Principal Place of Business in This State     | <input type="checkbox"/> 4 | <input checked="" type="checkbox"/> 4 |
| Citizen of Another State                | <input checked="" type="checkbox"/> 2 | <input type="checkbox"/> 2 | Incorporated and Principal Place of Business in Another State | <input type="checkbox"/> 5 | <input type="checkbox"/> 5            |
| Citizen or Subject of a Foreign Country | <input type="checkbox"/> 3            | <input type="checkbox"/> 3 | Foreign Nation  | <input type="checkbox"/> 6 | <input type="checkbox"/> 6            |

## IV. NATURE OF SUIT (Place an "X" in One Box Only)

CONTRACT	TORTS	FORFEITURE/PENALTY	BANKRUPTCY	OTHER STATUTES	
<input type="checkbox"/> 110 Insurance <input type="checkbox"/> 120 Marine <input type="checkbox"/> 130 Miller Act <input type="checkbox"/> 140 Negotiable Instrument <input type="checkbox"/> 150 Recovery of Overpayment & Enforcement of Judgment <input type="checkbox"/> 151 Medicare Act <input type="checkbox"/> 152 Recovery of Defaulted Student Loans (Excludes Veterans) <input type="checkbox"/> 153 Recovery of Overpayment of Veteran's Benefits <input checked="" type="checkbox"/> 160 Stockholders' Suits <input type="checkbox"/> 190 Other Contract <input type="checkbox"/> 195 Contract Product Liability <input type="checkbox"/> 196 Franchise	<b>PERSONAL INJURY</b> <input type="checkbox"/> 310 Airplane <input type="checkbox"/> 315 Airplane Product Liability <input type="checkbox"/> 320 Assault, Libel & Slander <input type="checkbox"/> 330 Federal Employers' Liability <input type="checkbox"/> 340 Marine <input type="checkbox"/> 345 Marine Product Liability <input type="checkbox"/> 350 Motor Vehicle <input type="checkbox"/> 355 Motor Vehicle Product Liability <input type="checkbox"/> 360 Other Personal Injury <input type="checkbox"/> 362 Personal Injury - Medical Malpractice	<b>PERSONAL INJURY</b> <input type="checkbox"/> 365 Personal Injury - Product Liability <input type="checkbox"/> 367 Health Care/Pharmaceutical Personal Injury Product Liability <input type="checkbox"/> 368 Asbestos Personal Injury Product Liability <b>PERSONAL PROPERTY</b> <input type="checkbox"/> 370 Other Fraud <input type="checkbox"/> 371 Truth in Lending <input type="checkbox"/> 380 Other Personal Property Damage <input type="checkbox"/> 385 Property Damage Product Liability	<input type="checkbox"/> 625 Drug Related Seizure of Property 21 USC 881 <input type="checkbox"/> 690 Other <b>LABOR</b> <input type="checkbox"/> 710 Fair Labor Standards Act <input type="checkbox"/> 720 Labor/Management Relations <input type="checkbox"/> 740 Railway Labor Act <input type="checkbox"/> 751 Family and Medical Leave Act <input type="checkbox"/> 790 Other Labor Litigation <input type="checkbox"/> 791 Employee Retirement Income Security Act	<input type="checkbox"/> 422 Appeal 28 USC 158 <input type="checkbox"/> 423 Withdrawal 28 USC 157 <b>PROPERTY RIGHTS</b> <input type="checkbox"/> 820 Copyrights <input type="checkbox"/> 830 Patent <input type="checkbox"/> 840 Trademark <b>SOCIAL SECURITY</b> <input type="checkbox"/> 861 HIA (1395ff) <input type="checkbox"/> 862 Black Lung (923) <input type="checkbox"/> 863 DIWC/DIWW (405(g)) <input type="checkbox"/> 864 SSID Title XVI <input type="checkbox"/> 865 RSI (405(g))	<input type="checkbox"/> 375 False Claims Act <input type="checkbox"/> 400 State Reapportionment <input type="checkbox"/> 410 Antitrust <input type="checkbox"/> 430 Banks and Banking <input type="checkbox"/> 450 Commerce <input type="checkbox"/> 460 Deportation <input type="checkbox"/> 470 Racketeer Influenced and Corrupt Organizations <input type="checkbox"/> 480 Consumer Credit <input type="checkbox"/> 490 Cable/Sat TV <input type="checkbox"/> 850 Securities/Commodities/Exchange <input type="checkbox"/> 890 Other Statutory Actions <input type="checkbox"/> 891 Agricultural Acts <input type="checkbox"/> 893 Environmental Matters <input type="checkbox"/> 895 Freedom of Information Act <input type="checkbox"/> 896 Arbitration <input type="checkbox"/> 899 Administrative Procedure Act/Review or Appeal of Agency Decision <input type="checkbox"/> 950 Constitutionality of State Statutes
<b>REAL PROPERTY</b> <input type="checkbox"/> 210 Land Condemnation <input type="checkbox"/> 220 Foreclosure <input type="checkbox"/> 230 Rent Lease & Ejectment <input type="checkbox"/> 240 Torts to Land <input type="checkbox"/> 245 Tort Product Liability <input type="checkbox"/> 290 All Other Real Property	<b>CIVIL RIGHTS</b> <input type="checkbox"/> 440 Other Civil Rights <input type="checkbox"/> 441 Voting <input type="checkbox"/> 442 Employment <input type="checkbox"/> 443 Housing/Accommodations <input type="checkbox"/> 445 Amer. w/Disabilities - Employment <input type="checkbox"/> 446 Amer. w/Disabilities - Other <input type="checkbox"/> 448 Education	<b>PRISONER PETITIONS</b> <input type="checkbox"/> Habeas Corpus: <input type="checkbox"/> 463 Alien Detainee <input type="checkbox"/> 510 Motions to Vacate Sentence <input type="checkbox"/> 530 General <input type="checkbox"/> 535 Death Penalty <input type="checkbox"/> Other: <input type="checkbox"/> 540 Mandamus & Other <input type="checkbox"/> 550 Civil Rights <input type="checkbox"/> 555 Prison Condition <input type="checkbox"/> 560 Civil Detainee - Conditions of Confinement	<b>FEDERAL TAX SUITS</b> <input type="checkbox"/> 870 Taxes (U.S. Plaintiff or Defendant) <input type="checkbox"/> 871 IRS—Third Party 26 USC 7609		
			<b>IMMIGRATION</b> <input type="checkbox"/> 462 Naturalization Application <input type="checkbox"/> 465 Other Immigration Actions		

## V. ORIGIN (Place an "X" in One Box Only)

- ☒ 1 Original Proceeding  
☐ 2 Removed from State Court  
☐ 3 Remanded from Appellate Court  
☐ 4 Reinstated or Reopened  
☐ 5 Transferred from Another District (specify)  
☐ 6 Multidistrict Litigation

## VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing (Do not cite jurisdictional statutes unless diversity):  
28 U.S.C. §1332

Brief description of cause:

Shareholder Derivative Action for Breach of Fiduciary Duty and Waste of Corporate Assets

## VII. REQUESTED IN COMPLAINT:

☐ CHECK IF THIS IS A CLASS ACTION UNDER RULE 23, F.R.Cv.P.

DEMAND \$

CHECK YES only if demanded in complaint:

JURY DEMAND: ☒ Yes ☐ No

## VIII. RELATED CASE(S) IF ANY

(See instructions):

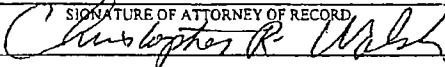
JUDGE Susan Richard Nelson

DOCKET NUMBER 0:14-cv-02203-SRN-JSM

DATE  
01/28/2014

FOR OFFICE USE ONLY

SIGNATURE OF ATTORNEY OF RECORD



RECEIPT #

AMOUNT

APPLYING IFP

JUDGE

MAG. JUDGE

JS 44 Reverse (Rev. 12/12)

**INSTRUCTIONS FOR ATTORNEYS COMPLETING CIVIL COVER SHEET FORM JS 44****Authority For Civil Cover Sheet**

The JS 44 civil cover sheet and the information contained herein neither replaces nor supplements the filings and service of pleading or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. Consequently, a civil cover sheet is submitted to the Clerk of Court for each civil complaint filed. The attorney filing a case should complete the form as follows:

- I.(a) **Plaintiffs-Defendants.** Enter names (last, first, middle initial) of plaintiff and defendant. If the plaintiff or defendant is a government agency, use only the full name or standard abbreviations. If the plaintiff or defendant is an official within a government agency, identify first the agency and then the official, giving both name and title.
- (b) **County of Residence.** For each civil case filed, except U.S. plaintiff cases, enter the name of the county where the first listed plaintiff resides at the time of filing. In U.S. plaintiff cases, enter the name of the county in which the first listed defendant resides at the time of filing. (NOTE: In land condemnation cases, the county of residence of the "defendant" is the location of the tract of land involved.)
- (c) **Attorneys.** Enter the firm name, address, telephone number, and attorney of record. If there are several attorneys, list them on an attachment, noting in this section "(see attachment)".
- II. **Jurisdiction.** The basis of jurisdiction is set forth under Rule 8(a), F.R.Cv.P., which requires that jurisdictions be shown in pleadings. Place an "X" in one of the boxes. If there is more than one basis of jurisdiction, precedence is given in the order shown below.
  - United States plaintiff. (1) Jurisdiction based on 28 U.S.C. 1345 and 1348. Suits by agencies and officers of the United States are included here. United States defendant. (2) When the plaintiff is suing the United States, its officers or agencies, place an "X" in this box.
  - Federal question. (3) This refers to suits under 28 U.S.C. 1331, where jurisdiction arises under the Constitution of the United States, an amendment to the Constitution, an act of Congress or a treaty of the United States. In cases where the U.S. is a party, the U.S. plaintiff or defendant code takes precedence, and box 1 or 2 should be marked.
  - Diversity of citizenship. (4) This refers to suits under 28 U.S.C. 1332, where parties are citizens of different states. When Box 4 is checked, the citizenship of the different parties must be checked. (See Section III below; NOTE: federal question actions take precedence over diversity cases.)
- III. **Residence (citizenship) of Principal Parties.** This section of the JS 44 is to be completed if diversity of citizenship was indicated above. Mark this section for each principal party.
- IV. **Nature of Suit.** Place an "X" in the appropriate box. If the nature of suit cannot be determined, be sure the cause of action, in Section VI below, is sufficient to enable the deputy clerk or the statistical clerk(s) in the Administrative Office to determine the nature of suit. If the cause fits more than one nature of suit, select the most definitive.
- V. **Origin.** Place an "X" in one of the six boxes.
  - Original Proceedings. (1) Cases which originate in the United States district courts.
  - Removed from State Court. (2) Proceedings initiated in state courts may be removed to the district courts under Title 28 U.S.C., Section 1441. When the petition for removal is granted, check this box.
  - Remanded from Appellate Court. (3) Check this box for cases remanded to the district court for further action. Use the date of remand as the filing date.
  - Reinstated or Reopened. (4) Check this box for cases reinstated or reopened in the district court. Use the reopening date as the filing date.
  - Transferred from Another District. (5) For cases transferred under Title 28 U.S.C. Section 1404(a). Do not use this for within district transfers or multidistrict litigation transfers.
  - Multidistrict Litigation. (6) Check this box when a multidistrict case is transferred into the district under authority of Title 28 U.S.C. Section 1407. When this box is checked, do not check (5) above.
- VI. **Cause of Action.** Report the civil statute directly related to the cause of action and give a brief description of the cause. Do not cite jurisdictional statutes unless diversity. Example: U.S. Civil Statute: 47 USC 553 Brief Description: Unauthorized reception of cable service
- VII. **Requested in Complaint.** Class Action. Place an "X" in this box if you are filing a class action under Rule 23, F.R.Cv.P. Demand. In this space enter the actual dollar amount being demanded or indicate other demand, such as a preliminary injunction. Jury Demand. Check the appropriate box to indicate whether or not a jury is being demanded.
- VIII. **Related Cases.** This section of the JS 44 is used to reference related pending cases, if any. If there are related pending cases, insert the docket numbers and the corresponding judge names for such cases.

**Date and Attorney Signature.** Date and sign the civil cover sheet.

**UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF MINNESOTA**

MAUREEN COLLIER, Derivatively on  
Behalf of TARGET CORPORATION,

Plaintiff,

v.

GREGG W. STEINHAFEL, JOHN J.  
MULLIGAN, BETH M. JACOB, JAMES A.  
JOHNSON, SOLOMON D. TRUJILLO,  
ANNE M. MULCAHY, ROXANNE S.  
AUSTIN, CALVIN DARDEN, MARY E.  
MINNICK, DERICA W. RICE, JOHN G.  
STUMPF, DOUGLAS M. BAKER, JR.,  
HENRIQUE DE CASTRO, and KENNETH L.  
SALAZAR,

Defendants,

-and-

TARGET CORPORATION,

Nominal Defendant.

Case No.

**VERIFIED SHAREHOLDER  
DERIVATIVE COMPLAINT**

**JURY TRIAL DEMANDED**

Plaintiff Maureen Collier ("Plaintiff"), by and through her attorneys, derivatively on behalf of nominal defendant Target Corporation ("Target" or the "Company"), submits this Verified Shareholder Derivative Complaint against the directors and officers named herein (collectively, the "Individual Defendants"). Plaintiff's allegations are based upon personal knowledge as to herself and her own acts, and upon information and belief developed from the investigation and analysis of her counsel, which includes, among other things, the review of public filings by Target with the U.S. Securities and Exchange Commission ("SEC"), as well as,

press releases, news reports, analyst reports, complaints pending against the Company, and other information available in the public domain.

### **SUMMARY OF THE ACTION**

1. This is a verified shareholder derivative action by Plaintiff on behalf of Target against certain of its officers and members of its Board of Directors (the “Board”), who are disabled from responding to a litigation demand by any Target shareholder because of their insider connections, tenure on the board, and involvement in the alleged wrongdoing for which they face a substantial likelihood of liability.

2. The Individual Defendants’ (as defined below) wrongful conduct extends at least from January 1, 2013 to the present (the “Relevant Period”). On behalf of Target, Plaintiff seeks monetary damages and injunctive relief by way of significant corporate and managerial reforms to prevent future harm to the Company by disloyal directors and officers.

3. Target trails Walmart as the second largest general merchandise retailer in the United States. Target allows customers to pay for goods using a variety of methods. A key method of payment in the digital age is via credit or debit card. Credit and debit card purchases are common in Target stores and are the primary method of payment on Target’s website for online purchases. Additionally, Target derives a substantial portion of its business through its own proprietary Target credit cards. To complete these transactions, Target routinely collects its customers’ personal and financial information. In addition to the information needed to complete a financial transaction, Target also collects vast amounts of other personal information about its customers, even tracking their purchase history to preemptively market potential future purchases. Customers are generally unaware that most of this information is collected and



retained. For the information that customers do willingly submit to complete a purchase, Target assures its customers that it will protect its sensitive and private nature.

4. This action arises out of the Individual Defendants' responsibility for, release of false and misleading statements concerning, and the bungling of the aftermath of the *worst data breach in retail history*.<sup>1</sup> The Individual Defendants caused Target to violate its express and implied promises to customers by failing to take reasonable steps to maintain its customers' personal and financial information in a secure manner.

5. When the Individual Defendants first revealed the breach, they significantly downplayed its true significance. The initial response from Target was that the breach only concerned data taken from the forty million customers who made credit and debit card purchases in physical Target stores nationwide between November 27 and December 15, 2013. The Individual Defendants also withheld from the public the news of the breach until after the 2013 Holiday Shopping Season in order to preserve sales figures during the most popular shopping period of the fiscal year. The fact that the Individual Defendants withheld the truth about the breach, put millions more customers at risk and had the effect of significantly increasing the damage to Target's goodwill and brand trust.

6. Almost a month after the breach, Target revealed the whole story. Namely, as a result of the Individual Defendants' failure to enact appropriate security measures, identity thieves were able to steal sensitive personal and financial data from as many as one hundred ten million customers who had shopped at Target over the last decade. The Individual Defendants' lack of controls effectively turned the vast majority of Target customers into victims of identity theft.

---

<sup>1</sup> 'Worst breach in history' puts data-security pressure on retail industry, CNBC, <http://www.cnbc.com/id/101328596>

7. Identity theft occurs when a thief wrongfully obtains a victim's personal information, without the victim's knowledge, to commit theft or fraud. For many of these victims, identity thieves have already used this personal information to commit fraud and other crimes. The remaining victims are forced to constantly wait and monitor financial and personal records to protect themselves from the threat of identity theft and fraudulent charges being made to their credit and debit card accounts that Target failed to keep safe.

8. In addition to being the *worst breach in history*, the Individual Defendants aggravated the damage to customers by failing to provide prompt and adequate notice to customers and by releasing numerous statements aimed to create a false sense of security to affected customers. Initially, the Individual Defendants allowed Target to delay admitting the breach to the public until December 19, 2013, several weeks after the breach began and four whole days after it had been contained. Worse, Target disclosed the data breach only after its hand was forced by third-party reports breaking the news. Still, after these mistakes, Target concealed the full breadth and depth of the data breach. In particular, Target initially reported on December 19, 2013 that the data breach affected forty million people and assured those affected by the data breach that "the issue has been identified and resolved," and that there was "no indication that there has been any impact to PIN numbers." Target further reassured worried customers that "someone cannot visit an ATM with a fraudulent debit card and withdraw cash." In fact, Target tried to preserve holiday sales figures and store traffic despite the negative news by offering all customers a 10% discount during the weekend of December 21 and 22, 2013, immediately following the initial disclosure of the breach.

9. Despite these statements to the contrary, just days after Target's initial disclosure of the data breach, news outlets began reporting that encrypted PIN (or personal identification

number) data had been stolen during the breach and that those codes could be used by identity thieves to make fraudulent withdrawals from bank accounts. In response to these allegations, Target continued for several days to deny that any of its customers' PIN data had been compromised.

10. On December 27, 2013, Target finally admitted that customers' PIN data had been compromised in the breach. Following the pattern of initially withholding the full truth until forced to tell all by independent news sources, on January 10, 2014, Target released a statement indicating that the breach had actually affected seventy million additional customers who had shopped at Target over the past ten years, not just the short period during the 2013 holiday shopping season.

11. Even after Target came clean about the true nature and scope of the breach, its customers have not been able to rest easy. To quell customer fears about identity theft, Target began offering free credit monitoring services to affected customers in the aftermath of the breach. Because Target thought this capitulation would be a good press public relations opportunity, they widely disclosed the credit services. Shortly thereafter, another round of identity thieves capitalized on this new opportunity to exploit Target's customers. In addition to the official emails sent to Target customers, including the proper links to sign up for free credit monitoring, a wider swath of sham emails sent by credit predators was sent out to Target customers and many people who had never even shopped at Target. These emails bore uncanny resemblances to the official emails but had the inverse purpose. The sham emails instructed the recipients to pass along their credit information so that it could be "monitored," when in fact it was just being directly stolen. This secondary breach has further eroded Target's goodwill and customer confidence.

12. The Individual Defendants' failures to implement any internal controls at Target designed to detect and prevent such a data breach, and then to timely report it, have severely damaged the Company. The Company's data breach is currently under investigation by the United States Secret Service ("Secret Service") and the Department of Justice ("DOJ"). The breach is also the subject of hearings in the United States Senate. Defendant John J. Mulligan ("Mulligan"), the Company's Executive Vice President and Chief Financial Officer ("CFO") is scheduled to appear before the Senate Judiciary Committee on February 4, 2014 to answer questions about the worst data breach in history. Finally, there are currently at least nineteen class action lawsuits filed against Target on behalf of affected customers. These class action lawsuits pose the risk of hundreds of millions of dollars in damages to the Company. Plaintiff therefore seeks damages and other relief on behalf of the Company.

#### **JURISDICTION AND VENUE**

13. This Court has diversity jurisdiction over this action pursuant to 28 U.S.C. §1332. All defendants are completely diverse from the Plaintiff and the amount in controversy exceeds \$75,000.00.

14. This Court has personal jurisdiction over each of the defendants because each defendant is either a corporation conducting business and maintaining operations in this District, or is an individual who is either present in this District for jurisdictional purposes or has sufficient minimum contacts with this District so as to render the exercise of jurisdiction by this Court permissible under traditional notions of fair play and substantial justice.

15. Venue is proper in this District pursuant to 28 U.S.C. §1391 because (i) one or more of the defendants either resides or maintains executives offices in the District; (ii) a substantial portion of the transactions and wrongs complained of herein occurred in the District;

and (iii) defendants have received substantial compensation and other transfers of money in the District by doing business and engaging in activities having an effect in the District.

### **PARTIES**

#### **Plaintiff**

16. Plaintiff is presently a shareholder of Target. Plaintiff has been a shareholder continuously at all times relevant to the claims asserted herein and will remain a shareholder through the conclusion of this litigation. Plaintiff is a citizen of Florida.

#### **Nominal Defendant**

17. Nominal Defendant Target is a Minnesota corporation with principal executive offices located at 1000 Nicollet Mall, Minneapolis, Minnesota 55440. Target is publicly traded on the New York Stock Exchange under the ticker symbol TGT.

#### **Individual Defendants**

18. Defendant Gregg W. Steinhafel (“Steinhafel”) has served as Target’s Chief Executive Officer (“CEO”) since May 2008; President since August 1999; Chairman of the Board since February 2009; and director since 2007. Defendant Steinhafel has been employed by Target since 1979. Defendant Steinhafel is a citizen of Minnesota.

19. Defendant Mulligan has served as Target’s Executive Vice President and CFO since April 1, 2012. Defendant Mulligan has served Target in key leadership positions in finance and human resources for over sixteen years. Defendant Mulligan is a citizen of Minnesota.

20. Defendant Beth M. Jacob (“Jacob”) has served as Target’s Chief Information Officer since July 2008 and Executive Vice President - Target Technology Services since January 2010. Defendant Jacob also served as Senior Vice President - Target Technology Services from July 2008 to January 2010 and Vice President - Guest Operations, Target Financial Services from August 2006 to July 2008. Defendant Jacob is a citizen of Minnesota.

21. Defendant James A. Johnson (“Johnson”) has served as Target’s Lead Independent Director since April 2012 and as director since 1996. Defendant Johnson has also served as a member of Target’s Corporate Responsibility Committee since April 2012. Defendant Johnson is a citizen of Washington, D.C.

22. Defendant Solomon D. Trujillo (“Trujillo”) has served as a Target director since 1994. Defendant Trujillo has also served as Chairman of Target’s Corporate Responsibility Committee since April 2012. Defendant Trujillo is a citizen of California.

23. Defendant Anne M. Mulcahy (“Mulcahy”) has served as a Target director since 1997. Defendant Mulcahy has also served as a member of Target’s Audit Committee since at least January 2014. Defendant Mulcahy is a citizen of Connecticut.

24. Defendant Roxanne S. Austin (“Austin”) has served as a Target director since 2002. Defendant Austin has also served as Chairman of Target’s Audit Committee since April 2012. Defendant Austin is a citizen of California.

25. Defendant Calvin Darden (“Darden”) has served as a Target director since 2003. Defendant Darden has also served as a member of Target’s Corporate Responsibility Committee since at least January 2014. Defendant Darden is a citizen of Georgia.

26. Defendant Mary E. Minnick (“Minnick”) has served as a Target director since 2005. Defendant Minnick has also served as a member of Target’s Audit and Corporate Responsibility Committees since April 2012. Defendant Minnick is a citizen of the United Kingdom.

27. Defendant Derica W. Rice (“Rice”) has served as a Target director since 2007. Defendant Rice has also served as a member of Target’s Audit Committee since April 2012. Defendant Rice is a citizen of Indiana.

28. Defendant John G. Stumpf ("Stumpf") has served as a Target director since 2010. Defendant Stumpf also served as a member of Target's Audit Committee from at least April 2012 until March 2013. Defendant Stumpf is a citizen of California.

29. Defendant Douglas M. Baker, Jr. ("Baker") has served as a Target director since March 2013. Defendant Baker also served as a member of Target's Audit Committee from March 2013 to April 2013. Defendant Baker is a citizen of Minnesota.

30. Defendant Henrique De Castro ("De Castro") has served as a Target director since March 2013. Defendant De Castro has also served as a member of Target's Corporate Responsibility Committee since March 2013. Defendant De Castro is a citizen of California.

31. Defendant Kenneth L. Salazar ("Salazar") has served as a Target director since July 2013. Defendant Salazar has also served as a member of Target's Corporate Responsibility Committee since November 2013. Defendant Salazar is a citizen of Colorado.

32. The defendants referenced above in ¶¶18-31 are collectively referred to herein as the "Individual Defendants." The defendants referenced in ¶¶18-20 above are referred to herein as the "Officer Defendants." The defendants referenced in ¶¶18 and 21-31 above are referred to herein as the "Director Defendants."

#### **FIDUCIARY DUTIES OF THE INDIVIDUAL DEFENDANTS**

33. The Individual Defendants have stringent fiduciary obligations to Target and its shareholders.

34. By reason of their positions as officers, directors, and/or fiduciaries of Target and because of their ability to control the business and corporate affairs of Target, the Individual Defendants owed Target and its shareholders fiduciary obligations of trust, loyalty, good faith, and due care, and were and are required to use their utmost ability to control and manage Target in a fair, just, honest, and equitable manner. The Individual Defendants were and are required to

act in furtherance of the best interests of Target and not in furtherance of their personal interest or benefit.

35. Each director and officer of the Company owes to Target and its shareholders the fiduciary duty to exercise good faith, loyalty, and diligence in the administration of the affairs of the Company and in the use and preservation of its property and assets, and the highest obligations of fair dealing. In addition, as officers and/or directors of a publicly held company, the Individual Defendants have a duty to promptly disseminate accurate and truthful information with regard to the Company's true forecasts and business prospects.

36. The Individual Defendants, because of their positions of control and authority as directors and/or officers of Target, were able to, and did, directly and/or indirectly, exercise control over the wrongful acts complained of herein, as well as the contents of the statements made publicly available and other actions taken in the aftermath of the data breach. Because of their advisory, executive, managerial, and directorial positions with Target, each of the Individual Defendants had access to adverse, non-public information about the financial condition, operations, and improper practices and representations of Target.

37. At all times relevant hereto, each of the Individual Defendants was the agent of each of the other Individual Defendants and of Target, and was at all times acting within the course and scope of such agency.

38. To discharge their duties, the officers and directors of Target were required to exercise reasonable and prudent supervision over the management, policies, practices, and controls of the financial affairs of the Company. By virtue of such duties, the officers and directors of Target were required to, among other things:

- (a) refrain from acting upon material inside corporate information to benefit



themselves;

(b) ensure that the Company complied with its legal obligations and requirements, including acting only within the scope of its legal authority and disseminating truthful and accurate statements;

(c) conduct the affairs of the Company in an efficient, businesslike manner so as to make it possible to provide the highest quality performance of its business, to be in compliance with all applicable laws and rules, to avoid wasting the Company's assets, and to maximize the value of the Company's stock;

(d) devise and maintain a system of internal controls sufficient to ensure that the Company's customers' personal and financial information is protected;

(e) ensure that the Company timely and accurately informed customers regarding any breach of their personal and financial information;

(f) ensure that the Company was operated in a diligent, honest and prudent manner in compliance with all applicable laws, rules and regulations; and

(g) remain informed as to how Target conducted its operations, and, upon receipt of notice or information of imprudent or unsound conditions or practices, make reasonable inquiry in connection therewith, and take steps to correct such conditions or practices.

39. Each Individual Defendant, by virtue of his or her positions as a director and/or officer, owed to the Company and to its shareholders the fiduciary duties of loyalty, good faith, and the exercise of due care and diligence in the management and administration of the affairs of the Company, as well as in the use and preservation of its property and assets. The conduct of the Individual Defendants complained of herein involves a knowing and culpable violation of their obligations as directors and/or officers of Target, the absence of good faith on their part,

and a reckless disregard for their duties to the Company and its shareholders that the Individual Defendants were aware or should have been aware posed a risk of serious injury to the Company. The conduct of the Individual Defendants who were also officers and/or directors of the Company during the Relevant Period has been ratified by the remaining Individual Defendants who collectively comprised all of Target's Board during the Relevant Period.

40. The Individual Defendants breached their duties of loyalty and good faith by allowing the other Individual Defendants to cause, or by themselves causing, the Company to release false and misleading statements as detailed herein, by failing to properly oversee the Company's business and operations, and by failing to prevent the Individual Defendants from taking such illegal actions.

41. As members of the Board of the Company, the directors named herein as the Individual Defendants were themselves directly responsible for authorizing or permitting the authorization of, or failing to monitor, the practices which resulted in the worst data breach in American retail history and the dissemination of false and misleading statements regarding the scope of that breach as alleged herein. Each of the Individual Defendants had knowledge of, actively participated in, and approved of the wrongdoings alleged or abdicated his responsibilities with respect to these wrongdoings. The alleged acts of wrongdoing subjected the Company to unreasonable risk of loss, and have resulted in large losses to the Company.

42. By reason of their positions of control and authority as officers and/or directors of Target, the Individual Defendants were able to and did, directly or indirectly, cause the Company to engage in and/or permit the conduct complained of herein. The Individual Defendants also failed to prevent the other Individual Defendants from taking such illegal actions. As a result,

and in addition to the damage the Company has already incurred, Target has expended, and will continue to expend, significant sums of money.

43. Moreover, Target maintains a Business Conduct Guide (hereafter the “Guide”), which applies to “all Target board members and to team members at every level and every location of Target and its operating divisions and subsidiaries.” The purpose of the Guide is to “to give [Target board members and employees] some tools to make decisions that reflect Target’s commitment to exemplary corporate ethics and integrity.” The Guide states in relevant part:

**OUR COMMITMENT TO COMPLIANCE**

Target has many teams dedicated to ensuring our business complies with all applicable laws and regulations. Complying with the requirements that govern our activities is vital to advancing our reputation. But the responsibility to drive compliance doesn’t just belong to specific teams within the company. **It belongs to you!** In fact, every team member, in every part of the organization, plays a role in compliance: from the business partner at headquarters making sure that our prices are accurate, to the warehousing team member at the distribution center staying current on the training requirements for her job, the pharmacy technician protecting guests’ medical information, or the ETL removing expired products from our shelves. All of these team members help Target comply with its regulatory obligations.

Best practices, policies, and procedures are some of the tools designed to enable Target to achieve its commitment to compliance. You are responsible for understanding these tools and knowing how and when to use them. If you’re unsure about what’s expected of you, talk with your supervisor to learn what to do. We take compliance very seriously and no one should dismiss the responsibility to meet these requirements. This guide is about the integrity and high ethical standards that are part of Target’s culture: the cornerstone of these attributes is our team members’ dedication to and ownership of compliance.

\*\*\*

*6 Protecting Target’s Assets*

**USE AS DIRECTED**

Target’s assets—no matter whether they’re merchandise, vendor samples, corporate credit cards, cash or information—are intended to be used for the benefit of the company. Target has accounting, reporting and internal controls and

teams in place to detect theft, fraud or misuse of company assets. When theft does occur, we investigate and resolve each incident quickly.

It's a pretty good bet that you already know your role in protecting Target's assets. If you don't, read the company's policies. If you see somebody stealing, or if you become aware of misuse of company assets, **alert your supervisor, Assets Protection or the Employee Relations and Integrity Hotline.**

#### *7 Record Retention*

##### **TO KEEP OR NOT TO KEEP?**

Many of us collect a lot of information in the course of doing our jobs—e-mails, memos, spreadsheets, contracts, proposals, project plans...the list goes on and the documents stack up. If you don't know how long you're supposed to keep that information, you risk keeping it too long or getting rid of it too soon. Cleaning out your files might result in discarding information that we need to keep, while keeping documents too long can result in confusion and an overstuffed electronic archive.

We have an obligation to ensure that our records are kept for the required amount of time. **Talk to your supervisor** to be sure that you understand the legal requirements and company expectations for keeping documents for which you're responsible, and the right way to dispose of documents we're no longer required to keep. You can also **contact Records Management** for a copy of our corporate records retention schedule.

\*\*\*

#### *9 Advertising*

##### **SAY IT PLAIN**

Guests are loyal to Target because they trust us to bring them high-quality merchandise at a good value, and to be a partner in building healthy communities. We've built that trust over decades, but we can damage it in an instant if we tell our guests something that turns out not to be true.

That's why our goal is clarity and accuracy in every advertisement we run. The claims made have to be true and supported; prices have to be accurate; we strive to have advertised merchandise available for guests to buy; and if the merchandise doesn't live up to guest expectations, we need to abide by our return policy. It's all about maintaining Target's brand and reputation.

\*\*\*

#### *12 Credit and Financial Services*

##### **THE RULES ARE THE RULES**

We offer credit to our guests through the Target® VISA® card, the REDcard® (both issued by Target National Bank), and the Target Business Card® (issued by

Target Bank). Other Target financial products include the Target GiftCard®, the Target Debit Card™ and the Target® Visa® Gift Card.

The state and federal laws and regulations that apply to consumer financial products and services run to thousands of pages. They govern everything from how we advertise our financial products and how we disclose product terms to how we manage cardholders' accounts and collect on past-due balances. There are even laws restricting how Target GiftCards can be displayed in our stores. If you're involved in creating, marketing or managing any of our financial products, you're responsible for following the designated procedures to meet our compliance obligations.

\*\*\*

#### *20 Financial Integrity and Reporting*

##### **FOR THE RECORD**

Target keeps records that reflect our financial statements and transactions with complete accuracy, and is committed to providing full, fair, accurate, timely and understandable disclosure in its external communications. The U.S. Securities and Exchange Commission and other governing bodies have strict rules about the accuracy of our financial statements and disclosures and about the strength of our internal controls over financial reporting. The Target Assurance team checks our internal controls periodically, and an outside auditor also checks the accuracy of our financial statements and disclosures. If anyone ever asks you to falsify a financial record, tell your supervisor, call the **Employee Relations and Integrity Hotline** or e-mail **Integrity@Target.com** right away—and remember that Target prohibits retaliation against any team member who makes a report in good faith.

44. In addition to these sections of the Guide that describe basic duties tangential to protecting customer personal and financial information, the Guide also contains a section that directly applies to the Individual Defendants' duties with regard to the personal and financial information of customers. That section of the Guide reads as follows:

#### *18 Information Protection and Privacy*

##### **PAUSE, PROTECT, PROCEED**

When guests share their personal information with us—like their names and addresses, credit card numbers and Social Security numbers—they expect Target to keep that information safe. If we break that trust, we'll damage Target's reputation and our relationship with guests. If someone asks you to share information, verify that they are who they say they are and that they're authorized to have the information they want.

No matter which area of Target you work in, you have access to information that could impact the reputation or financial well-being of Target, our guests and our team members if it falls into the wrong hands. Whether you work with protected health information, team-member information or business information such as price points, merchandise allocation, non-public financial information or company initiatives, you're entrusted to ensure that only people with a business need have access to the information you create, share and store.

All Target team members are expected to know and follow our Information Protection Policy. The policy outlines how information is classified at Target and how you should protect the information you work with throughout its life cycle. Target is subject to laws that require us to protect certain types of information and specify how that information should be protected.

When you're working with any kind of information, you should:

**Pause to understand its classification.** Target classifies information according to its level of sensitivity.

- **Secure Handling Required (SHR)** requires the highest levels of protection
- **Confidential** requires a high level of protection
- **Internal** can be shared with Target team members, contractors and authorized business partners
- **Public** can only be classified as such by only team members authorized to approve the release of information outside of Target

**Protect** information as required.

- Store data in a location accessible only to those who have a business need to know.
- Share data only with team members or vendors who need the information to do their jobs.
- Before sharing data with a vendor, ensure that the vendor has completed any necessary risk assessments and signed a confidentiality agreement with Target.
- Send data via secure methods according to its classification.
- Consult retention guides and schedules to know how long data needs to be stored and when it should be destroyed.
- Ensure that information is disposed of properly and according to its classification.

**Proceed** wisely according to the classification of the information you are using and the protection it requires.

Ask yourself: Is it okay for me to collect or share this information? Can the other team members or vendors I'm working with do their jobs without this information?

Want more detail? **Read the Target Information Protection Policy** or e-mail **Integrity@Target.com**

*Getting personal? Get the fine print right. When the Target Marketing team came up with the idea for a new campaign that would ask guests to register online and provide some personal information, they wanted to reassure guests—so they included language that said Target would use the collected information only for that specific campaign. But when Marketing checked with the Target Law department about how the language should read, they decided that definitive statements like the one Marketing proposed could conflict with Target's legal obligations, published privacy policies, or internal policies and practices. Target's Law team helped Marketing rewrite the language to make sure it was accurate and consistent with our policies.*

The ways in which Target collects, uses and shares guests' and team members' personal information all fall under the umbrella of "data privacy." Not only do we comply with applicable laws and regulations about how we handle guests' financial information and guests' and team members' health information, we've also created privacy policies that cover specific types of information (e.g., bank data and medical records) as well as a comprehensive privacy policy that covers collection, use and sharing of guest information. Some of our policies give guests and team members options for how their information will be used or shared.

If your job involves guests' or team members' personal information, it's important for you to **be aware of these policies and know how they apply to your work**. And it's equally important to consider these policies if we want to share guest or team-member information not just with third parties outside of Target, but also when we share information between Target affiliates like Target Stores and Target National Bank.

Ask yourself: Is there a privacy policy that applies to the information that I want to use or share?

Want more detail? E-mail [Integrity@Target.com](mailto:Integrity@Target.com).

45. Similarly, the members of the Audit Committee—Defendants Austin, Minnick, Mulcahy, and Rice—are governed by the rules set forth in the Audit Committee Position Description (hereafter the "Audit Committee Charter"). The Audit Committee Charter states that one function of the Audit Committee is "[t]o assist the Board of Directors in monitoring the integrity of the Corporation's financial statements, the independence, qualifications and performance of the Corporation's independent auditor, the performance of the Corporation's

internal audit function, the Corporation's compliance with legal and regulatory requirements and to approve the Committee's report for inclusion in the Corporation's Proxy Statement."

46. To that end, the Audit Committee's primary responsibilities and duties include, among other things, to:

**RESPONSIBILITIES:**

**A. Accounting and Reporting**

**1. Review of Press Releases and Other Information.** Discuss the Corporation's earnings press releases (including the use of "pro forma" or "adjusted" non-GAAP information), as well as financial information and earnings guidance provided to analysts and ratings agencies (discussion may be done generally and need not occur prior to each release).

\*\*\*

**4. Internal Controls - General.** Receive information from management about any significant deficiencies or material weaknesses in the design or operation of internal controls that could adversely affect the Corporation's ability to record, process, summarize and report financial data and any fraud, whether or not material, that involves management or other employees who have a significant role in the Corporation's internal controls. The Committee shall also review the independent auditor's letter reporting the status of internal controls and other matters the independent auditor considers appropriate and obtain and review management's response and corrective action plan.

\*\*\*

**6. General Oversight.** Discuss with management and the independent auditor significant financial reporting issues and judgments made in connection with the preparation of the Corporation's financial statements, including any significant changes in the Corporation's selection or application of accounting principles and any critical accounting estimates made in the course of preparing the financial statements.

\*\*\*

**D. Compliance Oversight**

**1. General.** Oversee the Corporation's ethics and compliance programs, including its Business Conduct Guide, and receive periodic reports on such programs from appropriate members of management.

**2. Investigations.** Conduct any investigation that the Committee deems appropriate, with full access to all of the Corporation's records, facilities,



personnel and outside advisors, and retain outside counsel, auditors and other consultants to advise the Committee for that purpose or others. The Corporation shall provide appropriate funding, as determined by the Committee, for payment of any resource engaged for this purpose and for all other administrative expenses necessary for the Committee to carry out its duties.

**3. Accounting and Auditing Complaints.** Establish procedures for the receipt, retention and treatment of complaints received by the Corporation regarding accounting, internal accounting controls or audit matters, and the confidential, anonymous submission by employees of concerns regarding questionable accounting or auditing matters.

**4. Legal Matters.** Review periodic reports of the General Counsel on litigation and other legal matters that may have a material impact on the financial statements or the Corporation's internal controls.

47. In derogation of these duties, Defendants Austin, Minnick, Mulcahy, and Rice, the members of the Audit Committee, failed to adequately monitor the Company's press releases and compliance with data protection laws and regulations.

### **FACTUAL ALLEGATIONS**

#### **Background**

48. As the nation's second largest general merchandise retailer, Target operates 1,797 stores in the United States. The Company also expanded into Canada in March 2013, where it operates 124 stores. The Company operates through three reportable segments: the U.S. Retail segment, the U.S. Credit Card segment, and the Canadian segment. The U.S. Retail segment includes all of the Company's physical stores, online, and catalog stores in the United States; the Credit Card segment operates Target's branded proprietary credit cards; and the Canadian segment operates the Company's March 2013 foray into Canadian market.

49. Historically, Target has used its power as the number two retailer in the United States to lobby against new technologies that would enhance the security of credit and debit card transactions. Many stores in Europe and Canada use chip-based credit cards that are much harder to replicate than normal credit cards. In 2004, Target moved against the new cards out of

fear that they would slow checkout speeds. Advocates had hoped that Target would adopt the program prior to 2004, which would have likely led to widespread adoption in the U.S. Because Target opted against the enhanced security program, the U.S. is now purposefully targeted for criminal cyber-attacks because of its position as one of the last remaining developed countries that does not take advantage of the more secure technology.

50. Target maintains a "Privacy Policy," which explains that the Company routinely collects personal information from its customers including a customer's name, mailing address, e-mail address, phone number, driver's license number, and credit/debit card number. In addition, when customers use their debit cards to make a purchase at Target, just as when they make a purchase using a debit card anywhere, they are required to enter the PIN associated with their bank account. In the "Privacy Policy," Target promises its customers that it will, among other things:

...maintain administrative, technical and physical safeguards to protect your personal information. When we collect or transmit sensitive information such as a credit or debit card number, we use industry standard methods to protect that information.

51. Blatantly breaking its promise and violating its duties to protect its customers' sensitive personal and financial information, the Individual Defendants caused Target to allow the sensitive and private information of over one hundred ten million customers to be compromised. Target's widespread failure to protect its customers' critical personal and financial information exposed victims to identity theft and has significantly damaged Target.

52. Armed with a customer's personal and financial information, identity thieves can easily encode the victim's account information onto a blank card with a magnetic strip creating a counterfeit card that can be used to make fraudulent purchases. With the addition of a victim's

PIN, a thief can use the counterfeit card to withdraw money directly from that person's bank account at any ATM machine (or automated teller machine) in the world.

53. Identity thieves can further exploit their victims by using personal information in a vast varieties of ways, including to open new credit, bank, and utility accounts, get cash advances, make large purchases, receive medical treatment on the victim's health insurance, and obtain to a driver's license or passport. Once an identity has been stolen, reporting, identifying, monitoring, and repairing the victim's credit is a stressful, time-consuming, expensive, and cumbersome process. On top of the frustration of having to identify and close affected accounts and correct information in credit reports, the victims of identity theft often incur costs associated with defending themselves against collection actions brought by creditors. Victims also suffer damage to their credit score and an enhanced burden when seeking new credit. Moreover, victims of identity theft must continue to monitor their credit reports for several years because fraudulent acts may not take place several years, yet still remain possible. Early estimates show that a mass breach of this nature will likely cost approximately \$5.10 per card that was exposed. For a breach of this magnitude, the total costs may very well approach \$561 million to Target.

54. The significance of protecting personal and financial information has pushed the federal government to enact of copious privacy-related laws aimed toward protecting consumer information and disclosure requirements. This legislation includes: (i) the Gramm-Leach-Bliley Act (the Financial Services Modernization Act of 1999); (ii) the Fair Credit Reporting Act; (iii) the Fair and Accurate Credit Transactions Act; (iv) the Federal Trade Commission Act; (v) the Health Insurance Portability and Accountability Act; (vi) the Health Information Technology for Economic and Clinical Health Act; (vii) the Driver's Privacy Protection Act; (viii) the E-Government Act of 2002; (ix) the Social Security Act Amendments of 1990; (x) the Privacy Act

of 1974; and (xi) the Federal Information Security Management Act of 2002. The federal government also maintains the newly created Consumer Financial Protection Bureau, which was established as an independent federal agency holding the primary responsibility for regulating consumer protection with regard to financial products and services in the United States.

55. Identity theft perpetrated over the internet as a cyber-attack is becoming more and more common in the digital age. A series of recent major cyber-attacks striking American corporations has prompted warnings from federal officials. In fact, as recently as May 2013 ICS-Cert, a division of the Department of Homeland Security that monitors attacks on computer systems that run industrial processes, issued a warning that the government was “highly concerned about hostility against critical infrastructure organizations.”

56. The Individual Defendants were fully aware of the risk of a potential data breach. On August 27, 2007, Dr. Neal Krawetz, a data security expert working for Hacker Factor Solutions, issued a paper titled “Point-of-Sale Vulnerabilities.” The paper warned Target and its peer major national retailers about the possibility of a point-of-sale data breach. The paper laid out the exact areas of vulnerability and even used Target as an example of the potential ramifications of a point-of-sale data breach at a major retailer. Further, Dr. Krawetz’s paper estimated that as many as fifty-eight million card accounts could be compromised if Target’s point-of-sale system was compromised. This was a widely-read paper and the Individual Defendants were undoubtedly aware of its findings.

57. The Individual Defendants have even acknowledged the risk of a data breach, yet failed to take any action to prevent that risk from coming to fruition. In its 2012 Form 10-K filed with the SEC on March 20, 2013, Target included a risk disclosure stating that the Company was fully aware of the consequences of failing to keep customers’ data secure and that the Company

could be subject to costly government enforcement actions and private litigation. The relevant portion of the Form 10-K read as follows:

If we experience a significant data security breach or fail to detect and appropriately respond to a significant data security breach, we could be exposed to government enforcement actions and private litigation. In addition, our guests could lose confidence in our ability to protect their personal information, which could cause them to discontinue usage of REDcards, decline to use our pharmacy services, or stop shopping with us altogether. The loss of confidence from a significant data security breach involving team members could hurt our reputation, cause team member recruiting and retention challenges, increase our labor costs and affect how we operate our business.

#### **The Data Breach**

58. The data breach that took place in November and December 2013 compromised one hundred ten million Target customers' personal and financial data. Within days of the breach, millions of affected customers' financial and personal information was being sold on the black-market.

59. The first news of the data breach did not come from Target, but was broken by KrebsOnSecurity.com on December 18, 2013. The website dedicated to reporting cybercrime, published an article indicating the occurrence of a massive data breach at Target stores. According to the article, Target was investigating the possible theft of millions of customer credit card and debit card records beginning November 27, 2013, and extending as far as December 15, 2013. The breach was said to have occurred when thieves accessed the Company's customers' personal and financial data by penetrating Target's point-of-sale system.

#### **The Individual Defendants' False Statements to Customers**

60. Target's customers were entitled to have the information they entrusted to Target protected to the greatest extent possible. And in the unlikely event that the data was breached, Target's customers were entitled to immediate, full, and accurate notification of the data breach to help them mitigate the harm and avoid additional instances of fraud. Conversely, the

Individual Defendants, failed to take the appropriate steps to cause the Company to notify customers that their sensitive information had been obtained by nefarious individuals for nefarious purposes. In so doing, the Individual Defendants served to aggravate the damage to affected customers and the Company.

61. After numerous third-party sources spread the news of the data breach across the news media for twenty-four hours, Target finally public acknowledged that its security systems had been compromised and its customers' trust had been betrayed. On December 19, 2013, over three weeks after the data breach began and four days after it had been contained, Target finally admitted the breach to the public. The Company issued a brief statement in which it confirmed that it had been aware of unauthorized access to certain customers' credit and debit card data at the Company's U.S. stores. The statement read as follows:

**Target Confirms Unauthorized Access to Payment Card Data in U.S. Stores**

Issue has been identified and resolved

MINNEAPOLIS — December 19, 2013

Target today confirmed it is aware of unauthorized access to payment card data that may have impacted certain guests making credit and debit card purchases in its U.S. stores. Target is working closely with law enforcement and financial institutions, and has identified and resolved the issue.

"Target's first priority is preserving the trust of our guests and we have moved swiftly to address this issue, so guests can shop with confidence. We regret any inconvenience this may cause," said Gregg Steinhafel, chairman, president and chief executive officer, Target. "We take this matter very seriously and are working with law enforcement to bring those responsible to justice."

Approximately 40 million credit and debit card accounts may have been impacted between Nov. 27 and Dec. 15, 2013. Target alerted authorities and financial institutions immediately after it was made aware of the unauthorized access, and is putting all appropriate resources behind these efforts. Among other actions, Target is partnering with a leading third-party forensics firm to conduct a thorough investigation of the incident.

62. The Company's statement aims to minimize the impact of the breach, stating that "[a]pproximately 40 million credit and debit card accounts may have been impacted between Nov. 27 and Dec. 15, 2013." Later, this initial statement would prove to be untrue.

63. In a separate statement issued that same day by defendant Steinhafel, Target explained more of the details of exactly what information was compromised. Defendant Steinhafel's December 19, 2013 statement stated that the data breach "included customer name, credit or debit card number, and the card's expiration date and CVV [card verification value, the three numbers on the reverse side of Visa and MasterCard or the four smaller numbers on the front side of American Express cards]." Defendant Steinhafel's statement restated the claim that "[t]he unauthorized access may impact guests who made credit or debit card purchases in our U.S. stores from Nov. 27 to Dec. 15, 2013."

64. The next day, December 20, 2013, in a publicity stunt attempting to contain and minimize the public perception of the impact of the data breach, defendant Steinhafel declared to "have worked swiftly to resolve the incident" and concluded that, "there is no indication that PIN numbers have been compromised on affected bank issued PIN debit cards or Target debit cards." Defendant Steinhafel further assured frazzled customers that "[s]omeone cannot visit an ATM with a fraudulent debit card and withdraw cash." That same day, defendant Steinhafel issued a press release on behalf of Target announcing that "the issue has been identified and eliminated" and that the Company would provide free credit monitoring services to affected customers. In an effort to restore confidence in the Company and keep the news of the breach from destroying the last few days of the 2013 holiday shopping season, Target offered to extend its employees' discount of 10% to all customers who shopped in Target stores on the weekend of December 21 and 22, 2013.

65. From the moment they were informed of the breach, the Individual Defendants tried to minimize reports regarding the extent of the breach and to protect Target sales during the 2013 holiday shopping season, in spite of the fact that such efforts would only serve to further erode customer confidence when the truth was finally revealed and cause greater damage to Target's reputation, brand, and goodwill.

66. As expected, despite Target's attempts to dispel customers' concerns, news once again began to emerge that credit and debit card information stolen from Target was appearing for sale online. According to several sources, customer account information stolen from Target was being sold on the black market in batches of one million cards and fraudulent purchase activity had begun being reported by issuing banks.

67. With each passing day, independent sources began to find and reveal more of the true scope of the breach. On December 23, 2013, Target acknowledged that the Secret Service and the DOJ decided to participate in the investigation into the breach. Additionally, the Company stated that it had spoken with the attorneys general for Massachusetts, New York, Connecticut, and South Dakota concerning the breach. Those attorneys general have now been joined by counterparts in Illinois, California, Minnesota, and several other states to investigate the breach.

68. The following day, news came out that, despite prior statements by Target to the contrary, encrypted PIN data had been stolen during the original breach and that those codes could be used by thieves to make fraudulent withdrawals from the victims' bank accounts. In response to these allegations, Target continued to deny that any of its customers' PIN data had been compromised. Defendant Steinhafel maintained that "[t]here is no indication that PIN



numbers have been compromised on affected bank issued PIN debit cards or Target debit cards” and that “[s]omeone cannot visit an ATM with a fraudulent debit card and withdraw cash.”

#### **The True Scope of the Breach is Finally Revealed**

69. Then, on December 27, 2013, two days after Christmas and the conclusion of the 2013 holiday shopping season, Target finally admitted that customers’ PIN data had been compromised in the breach. On January 10, 2014, Target disclosed that 70 million customers’ personal information may also have been affected by the data breach, bringing the total of possible victims up to over one hundred ten million Target customers. Additionally, this new swath of victims did not consist of only those customers who had made purchases at physical Target stores between November 27 and December 15, 2013, it included all Target customers online and in-store spanning as far back as ten years.

#### **The Individual Defendants Failed to Implement Appropriate Security Measures**

70. On the Company’s website Target recognizes that its customers’ personal and financial information is highly sensitive and must be protected. The Company maintains a Privacy Policy, that gives the following promise regarding personal information:

We maintain administrative, technical and physical safeguards to protect your personal information. When we collect or transmit sensitive information such as a credit or debit card number, we use industry standard methods to protect that information.

71. There are currently at least nineteen class action lawsuits being brought by Target’s customers against the Company for the data breach. In defending against those suits, Target will likely try to prove that it had been fully compliant with industry standards and therefore had done all it could to protect against the breach. The most prominent of these industry standards is the PCI Data Security Standard (“PCI”). The PCI is an industry standard

for large retail institutions that accept credit card and debit card transactions, but it is far less than it is cracked up to be. The standard consists of twelve general requirements including:

1. Install and maintain a firewall configuration to protect cardholder data;
2. Do not use vendor-supplied defaults for system passwords and other security parameters;
3. Protect stored cardholder data;
4. Encrypt transmission of cardholder data across public networks;
5. Use and regularly update anti-virus software or programs;
6. Develop and maintain secure systems and applications;
7. Restrict access to cardholder data by business need to know;
8. Assign a unique ID to each person with computer access;
9. Restrict physical access to cardholder data;
10. Track and monitor all access to network resources and cardholder data;
11. Regularly test security systems and processes; and
12. Maintain a policy that addresses information security for all personnel.

72. Even if Target is found to be in compliance with PCI, there is growing concern that the standard is not adequate to protect consumers. The system has been criticized for fostering complacency among merchants that meet the standards and offering the merchants a means of avoiding blame.

73. Nevertheless, on December 23, 2013, USA Today reported that Target was likely not even in compliance with the low standard of PCI. The article stated:

Target's massive databreach took place just a few weeks before a set of payment card industry standards - known as PCI DSS 3.0 - were scheduled to go into effect. CyberTruth asked Nick Aceto, technology director at software vendor CardConnect, to supply some clarity.

CyberTruth: What does this latest databreach tell us about the efficacy of PCI?

Aceto: We can't say definitely that this breach is a failure of Target's PCI compliance, but based on what Target has said, it's very hard to believe that they were even PCI 2.0 compliant at the time of the breach.

A reason for thinking this is that the attack, involving an enormous amount of data, went on essentially unnoticed for 18 days. How were they not watching the network?

One of the PCI DSS requirements is that you monitor your logs and firewalls every day, looking for unusual activity. This monitoring involves file integrity

checks and changes to critical systems files. What's more - the chapter 6 software development life cycle requires the secure distribution and verification of payment applications.

Unusual activity isn't always abnormal, but the point of PCI is to monitor and verify that all activity is normal, while not letting distractions - like busy shopping days Black Friday and Cyber Monday, on which the breach occurred - detract from the monitoring effort.

74. The Individual Defendants knew or should have known that the Company had failed to meet industry standards with its security systems and left its technologies unreasonably vulnerable rendering its customers a target of attacks by nefarious third-parties. The Individual Defendants, however, failed to take corrective measures to update Target's systems and technologies. Target's deficiencies included the failure to maintain adequate backups and/or redundant systems; failure to encrypt data and/or establish adequate firewalls to handle a server intrusion contingency; and failure to provide prompt and adequate warnings of security breaches.

#### **The Aftermath of the Breach and its Lasting Effect**

75. Once the full scope of the data breach became clear, so did its historical significance. A January 11, 2014 NBC News article quoting Ken Stasiak, the CEO of cybersecurity company SecureState, called Target's breach "*the worst breach in history*." Mr. Stasiak went on to say, "It's 2014. We expect retailers of this magnitude to have better security, weigh their risks and spend the resources necessary to secure their data." Empirically, Target's breach is the worst in history because it concerned the data of over one hundred ten million customers, far outreaching the previous holder of the title, TJX Companies, Inc. (parent of TJMaxx, Marshall's, and HomeGoods) with a breach of forty-five million customers' information in 2007.

76. Target itself has suffered considerable damage from breach itself and the bungling of its aftermath. In response to events described above, market analysts such as Cowen and Co. have lowered ratings on Target and trimmed price expectations. Cowen had formerly targeted

Target's price for \$66 per share, but on January 21 reduced that number to \$47 per share. Target shares were trading above \$63.50 on December 18, 2013 before the news of the data breach and have fallen over 10.5% to \$57.60.

77. On top of the loss in market capitalization, the economic impact of the breach has been felt throughout Target. The Company announced on January 22, 2014 that it was cutting health coverage for part-time workers as well as laying-off 475 workers and eliminating 700 open positions.

78. Public backlash from the breach is also far from over. While the Individual Defendants have tried to control the public relations nightmare of the breach on their own terms, federal legislators are now stepping in to further shame the Company. Defendant Mulligan has been called to appear before the U.S. Senate Judiciary Committee on February 4. This will be the first time that Target will be forced to answer questions about the worst breach in history. Preparation for this hearing and whatever action comes out of it, will likely cost the Company great sums of money in addition to that already being spent to quell the financial damage caused by the breach.

#### **DERIVATIVE AND DEMAND FUTILITY ALLEGATIONS**

79. Plaintiff brings this action derivatively in the right and for the benefit of Target to redress injuries suffered, and to be suffered, by Target as a direct result of the Individual Defendants' breaches of fiduciary duty.

80. Plaintiff will adequately and fairly represent the interests of the Company and its shareholders in enforcing and prosecuting its rights.

81. Target is named as a nominal defendant in this case solely in a derivative capacity. This is not a collusive action to confer jurisdiction on this Court that it would not otherwise have. Plaintiff is and was a shareholder of Target at the time of the transgressions

complained of. Prosecution of this action, independent of the current Board of Directors, is in the best interests of the Company.

82. The wrongful acts complained of herein subject, and will continue to subject, Target to continuing harm because the adverse consequences of the actions are still in effect and ongoing.

83. The wrongful acts complained of herein were unlawfully concealed from Target's shareholders.

84. Throughout the Relevant Period, the Individual Defendants violated multiple corporate governance principles, thus representing evidence of the Individual Defendants' breaches of fiduciary duties. The course of action included failing to maintain appropriate data security systems and concealing the truth about the breach from the public, and caused the Individual Defendants to breach the following corporate principles, among others:

- a. protect customers' personal and financial information in accordance with the Privacy Policy, the Guide, and industry best practices;
- b. maintain a system of internal controls that will provide reasonable assurances to management that material information about the Company is made known to management, particularly information being conveyed by the Company that concerns the public trust; and
- c. comply with all local and federal laws and regulations.

85. As a result of the facts set forth herein, Plaintiff has not made any demand on the Target Board to institute this action since such demand would be a futile and useless act because the Board is incapable of making an independent and disinterested decision to institute and vigorously prosecute this action. The wrongful acts complained of herein show a wholesale

abandonment by the Individual Defendants of their fiduciary duties of due care, oversight, and loyalty. Such abandonment includes, but is not limited to the following:

- a. Allowing for materially inadequate controls over the Company's policies with respect to cyber-security and the protection of sensitive customer information;
- b. Allowing the Company to make false statements concerning the data breach and to withhold the breach from the affected customers; and
- c. Failing to adequately remedy the data breach in the fashion expected of the second largest retailer in the United States.

86. At the time of filing, the Board consisted of twelve individuals: Defendants Steinhafel, Johnson, Trujillo, Mulcahy, Austin, Darden, Minnick, Rice, Stumpf, Baker, De Castro, and Salazar. Plaintiff did not make any demand on the Board to institute this action because such a demand would be a futile, wasteful, and useless act, particularly for the following reasons:

- a. As a result of their access to and review of internal corporate documents, conversations and connections with other corporate officers, employees and directors; and attendance at management and the Board meetings during the Relevant Period, each of the Director Defendants knew, or were reckless in not knowing, that the Company was obscenely vulnerable to a cyber-security attack upon customers personal and financial information that would subject the Company to hundreds of millions of dollars in liability, yet failed to take any meaningful action to correct these problems and foster compliance with applicable laws and regulations; and

- b. The Director Defendants were particularly aware of the industry standards for secure transactions and new technologies that could have enhanced security and chose not to implement further security measures and to lobby against the widespread adoption of new technology.

87. Defendants Steinhafel, Johnson, Trujillo, Mulcahy, Austin, Darden, Minnick, Rice, Stumpf, Baker, De Castro, and Salazar, the Company's entire current Board, caused the Company to withhold and then disseminate improper, materially false and misleading public statements concerning, among other things, the true nature and extent of the data breach. Customers were entitled to adequate and prompt notification about the data breach to help them mitigate the harm and avoid additional instances of fraud. The Individual Defendants, however, failed to take reasonable steps to have the Company notify consumers that their information had been compromised. The Company's public disclosures concerning the data breach were improper because: (i) they were untimely and only released after third-party organizations began spreading the news; (ii) they understated the scope of the affected victims by seventy million people; (iii) they diminished the severity of the harm to customers by failing to disclose that PINs were compromised, (iv) withheld the scope of the personal data that was compromised, and (v) allowed for a secondary breach to occur in the aftermath of the initial breach in the form of fraudulent credit monitoring emails. Each member of the Board knew or should have known that the improper statements did not timely, fairly, accurately, or truthfully convey the scope of the data breach. In addition, when deciding whether to approve statements to be publicly disseminated, each member of the Board was bound by the duty of care and the duties set forth in the Guide to inform himself or herself of all reasonably-available material information. Information concerning the nature and extent of the data breach was both reasonably available

and material to members of the Board. Defendants Steinhafel, Johnson, Trujillo, Mulcahy, Austin, Darden, Minnick, Rice, Stumpf, Baker, De Castro, and Salazar's conduct can in no way be considered a valid exercise of business judgment. Accordingly, demand on the Board is excused as futile.

88. A majority of the Board is incapable of disinterestedly and independently considering a demand to commence and vigorously prosecute this action for the following reasons:

a. Defendants Steinhafel, Johnson, Trujillo, Mulcahy, Austin, Darden, Minnick, Rice, Stumpf, Baker, De Castro, and Salazar, are substantially likely to be held liable for breaching their fiduciary duties, gross mismanagement, abuse of control, and by maintaining inadequate internal control of information privacy and cyber-security as complained of herein.

b. Further, Defendants Steinhafel, Johnson, Trujillo, Mulcahy, Austin, Darden, Minnick, Rice, Stumpf, Baker, De Castro, and Salazar face a substantial likelihood of liability due to their failure to provide adequate and prompt notice to consumers and because they conveyed a false sense of security to customers affected by the data breach. Defendants Steinhafel, Johnson, Trujillo, Mulcahy, Austin, Darden, Minnick, Rice, Stumpf, Baker, De Castro, and Salazar breached their duty of loyalty by causing the Company to disseminate the improper public statements discussed herein. Accordingly, all the Board members face a substantial likelihood of liability, rendering demand upon them futile.

c. Defendant Steinhafel is both Target's CEO and President. Defendant Steinhafel is not disinterested because it is very likely that he will be held liable in any action brought on behalf of the corporation for his alleged wrongdoing. In fiscal year 2012, Defendant Steinhafel



received \$20,647,464 in compensation from Target. Due to his excessive compensation and position as an insider in the Company, he is entrenched in the Company.

d. Defendants Johnson, Trujillo, Mulcahy, Austin, Darden, Minnick, Rice, and Stumpf each received over \$250,000 in compensation for their service as directors in 2012. Due to their significant director compensation, Defendants Johnson, Trujillo, Mulcahy, Austin, Darden, Minnick, Rice, and Stumpf are disabled from impartially considering a demand to prosecute the claims herein.

e. Several of the Director Defendants have served long tenures as directors with the Company and cannot objectively appraise whether to pursue an action upon themselves and their colleagues. Defendant Johnson has served as a director since 1996. Defendant Trujillo has served as a director since 1994. Defendant Mulcahy has served as a director since 1997. Defendant Austin has served as a director since 2002. Defendant Darden has served as a director since 2003. Defendant Minnick has served as a director since 2005. Due to their long tenure and the close business relationships built up over nine-plus years of common service on the Target Board, defendants Johnson, Trujillo, Mulcahy, Austin, and Minnick are disabled from impartially and independently considering a demand to sue their fellow directors with whom they have established significant professional ties.

f. Defendants Austin, Minnick, Mulcahy, and Rice all served as members of the Audit Committee during the Relevant Period. Defendant Austin was and continues to be the Chairman of the Audit Committee. According to the Audit Committee Charter, Defendants Austin, Minnick, Mulcahy, and Rice have the specific duty to oversee all material aspects to the Company's reporting, control, and audit functions. Because they breached that duty, there is a high likelihood that they will be held personally liable in any litigation brought on behalf of the

Company. It is for this reason, among others, that the members of the Audit Committee are not disinterested and cannot reasonably decide whether to bring litigation against themselves on behalf of the Company.

89. During the Relevant Period the Individual Defendants caused or allowed the Company to fail to maintain proper internal controls over their security and privacy systems and to issue false and misleading statements when those systems were breached. The Individual Defendants' misconduct has severely damaged, and will continue to severely damage, the Company. Further, and more importantly, Target's reputation, goodwill, brand trust, and positive brand recognition have been tainted by the misconduct described herein.

90. As detailed above, the Board members were directly involved in the misconduct challenged in this action, by virtue of their respective positions on the Board and its Committees, and completely abdicated their responsibility to oversee the Company's operations, causing the Company to engage in illegal and/or improper conduct regarding cyber-security and the public statements and surrounding the breach, destroying in their wake, much of the Company's shareholder value. The Individual Defendants' conduct lacked any legitimate business purpose and was not a product of a valid exercise of business judgment. As such, demand is excused as futile.

91. The Individual Defendants' conduct described herein and summarized above demonstrates a pattern of misconduct that could not have been the product of legitimate business judgment as it was based on intentional, reckless, and disloyal misconduct. Thus, none of the Individual Defendants, who constitute the entire current Board of the Company, can claim exculpation from their violations of duty pursuant to the Company's Articles of Incorporation. As a majority of the Individual Defendants face a substantial likelihood of liability, they are self-

interested in the transactions challenged herein and cannot be presumed to be capable of exercising independent and disinterested judgment about whether to pursue this action on behalf of the shareholders of the Company. Accordingly, demand is excused as being futile.

92. Furthermore, the Target Board is still dominated and controlled by the exact same wrongdoers who continue to obscure their own misconduct, and will not take action to protect the interests of Target or its shareholders. The present Board has refused, and will continue to refuse, to institute this action for the foregoing and following reasons:

- a. The acts complained of herein constitute violations of fiduciary duties owed by the Board of Directors and these acts are incapable of ratification;
- b. Certain of the known principal wrongdoers and beneficiaries of the wrongdoing complained of herein are in a position to, and do, dominate and control the Board of Directors. Thus, the Board could not exercise independent objective judgment in deciding whether to bring or vigorously prosecute this action;
- c. The acts complained of herein are illegal and improper and thus are acts incapable of ratification;
- d. In order to bring this action for breach of fiduciary duty, the members of the Board of Directors would have been required to sue themselves and/or their fellow directors and allies in the top ranks of the Company, who have personal relationships and with whom they have entangling financial alliances, interests, and dependencies, which they would not do. They therefore would not be able to vigorously prosecute any such action; and

e. The members of the Target Board, including each of the Defendants herein, receive substantial salaries, bonuses, payments, benefits, and other emoluments by virtue of their membership on the Board and their control of Target. They have thus benefited from the wrongs herein alleged and have engaged therein to preserve their positions of control and the perquisites thereof, and are incapable of exercising independent objective judgment in deciding whether to bring this action. The Board members also have close personal or business ties with each other and are, consequently, interested parties and cannot in good faith exercise independent business judgment to determine whether to bring this action against themselves.

93. Moreover, each of the Individual Defendants, as an officer and/or director of Target, had intimate knowledge of all major operations of the Company, and yet participated in maintenance of inadequate cyber-security controls and the dissemination of material misstatements about the scope of the breach. Thus, the Individual Defendants all have a personal interest in concealing any blame for Target's internal controls problems, and shifting the blame away from themselves for consciously disregarding fiduciary duties. An investigation or inquiry that spread blame higher up the corporate ladder—to the Individual Defendants, as officers and/or directors—would not be in the personal interest of the Individual Defendants. The result of such an inquiry would require them to return valuable but unearned compensation to the Company.

94. In addition, all Individual Defendants face a sufficiently substantial likelihood of liability, and thus, there is a reasonable doubt as to each of their disinterestedness in deciding whether pursuing legal action would be in the Company's best interest.

95. Further, any suit by the current directors of Target to remedy these wrongs would expose Target to liability in the numerous pending consumer class actions lawsuits. There are currently no less than nineteen consumer class actions filed against the Company as a result of the data breach. These class actions allege various claims, including, but not limited to, negligence, breach of contract, and violation of state privacy laws. If the Board elects for the Company to press forward with its right of action against any of the members of the Board in this action, Target's efforts would directly compromise its defense of the pending consumer class actions. Accordingly, demand on the Board is excused as futile.

#### **DAMAGES TO THE COMPANY**

96. As a direct and proximate result of the Individual Defendants' misconduct, Target failed to maintain proper internal controls, caused the Company to release false and misleading statements, caused the Company to pay large sums of money for credit monitoring services for affected customers, caused the Company to be exposed to millions of dollars of potential liability in class action lawsuits, and substantially damaged the Company's sales during the 2013 holiday season, its market capitalization, goodwill, consumer confidence, and brand trust.

97. Furthermore, Target has expended and will continue to expend significant sums of money. Such expenditures include but are not limited to:

- a. costs incurred from the Company's internal investigation into the data breach, but not limited to, expense for legal, investigative, and consulting fees;
- b. costs of updating customers of the status of the breach;
- c. costs incurred from providing credit monitoring for 110 million affected customers;
- d. costs incurred from defending and settling the numerous class action lawsuits being brought against the Company for the breach;

- e. costs incurred from notifying customers, replacing cards, sorting improper charges from legitimate charges, and reimbursing customers for fraudulent transactions (early estimates put this at roughly \$5.10 per card, or \$561 million);
- f. costs incurred from the Secret Service, DOJ, and U.S. Senate investigations into the data breach, including, but not limited to, liability for any potential fines;
- g. costs incurred from notifying customers and rectifying secondary breach caused by imitation credit monitoring emails;
- h. loss of revenue and profit resulting from Target's offer of a 10% discount to U.S. shoppers during the last weekend before Christmas in an effort to lure customers back into its stores;
- i. costs incurred from instituting chip-based credit cards that will enhance security; and
- j. costs incurred from compensation and benefits paid to the defendants who have breached their duties to Target.

98. Moreover, these actions have irreparably damaged Target's corporate image and goodwill such that all Target stores and financial services are associated with failing to protect customer's sensitive information and then keeping that broken promise a secret from customers.

#### COUNT I

#### **DERIVATIVELY AGAINST ALL DEFENDANTS** **FOR BREACH OF FIDUCIARY DUTY**

99. Plaintiff incorporates by reference and re-alleges each and every allegation contained above, as though fully set forth herein.

100. The Individual Defendants owed and owe Target fiduciary obligations. By reason of their fiduciary relationships, the Individual Defendants owed and owe Target the highest obligation of loyalty, good faith, due care, oversight, fair dealing, and candor.

101. All of the Individual Defendants violated and breached their fiduciary duties of loyalty, good faith, due care, oversight, fair dealing, and candor.

102. Each of the Individual Defendants had actual or constructive knowledge that they had caused Target to maintain improper security controls of customer data and to make false and misleading statements about the data breach once it occurred. These actions could not have been a good faith exercise of prudent business judgment to protect and promote the Company's corporate interests.

103. The Individual Defendants caused or allowed Target to lack requisite internal controls, and, as a result, the Company allowed the worst data breach of customer information in retail history.

104. The Individual Defendants failed to supervise, and to ensure adequate internal controls over, and consciously disregarded responsibilities involving, the Company.

105. The Individual Defendants caused or allowed the scope of the breach to be materially misstated and misrepresented.

106. As a direct and proximate result of the Individual Defendants' failure to perform their fiduciary obligations, Target has sustained significant damages. As a result of the misconduct alleged herein, the Individual Defendants are liable to the Company.

## COUNT II

### **DERIVATIVELY AGAINST ALL DEFENDANTS** **FOR GROSS MISMANAGEMENT**

107. Plaintiff incorporates by reference and re-alleges each and every allegation contained above, as though fully set forth herein.

108. By their actions alleged herein, the Individual Defendants abandoned and abdicated their responsibilities and fiduciary duties with regard to prudently managing the assets and business of Target in a manner consistent with the operations of a publicly held corporation.

109. The Individual Defendants caused or allowed Target to lack requisite internal controls, and as a result, the Company allowed the worst data breach in retail history and then released a series of false and misleading statements about the gravity of the breach.

110. The Individual Defendants caused or allowed the Company's statements to be materially misstated due to the Individual Defendants' failure to properly account for the Company's motives of withholding information from the public in order to protect sales figures.

111. The Individual Defendants failed to supervise, and to exert internal controls over, and consciously disregarded responsibilities involving the Company's public statements, as well as the Company's cyber-security systems.

112. The Individual Defendants caused or allowed the scope of the breach to be materially misstated.

113. The Individual Defendants, including members of the Audit Committee, did not take seriously their primary responsibility for the Company's statistical and financial reporting activities.

114. As a direct and proximate result of the Individual Defendants' gross mismanagement and breaches of duty alleged herein, Target has sustained significant damages that will likely exceed hundreds of millions of dollars.



115. As a result of the misconduct and breaches of duty alleged herein, the Individual Defendants are liable to the Company.

**COUNT III**

**DERIVATIVELY AGAINST ALL DEFENDANTS**  
**FOR WASTE OF CORPORATE ASSETS**

116. Plaintiff incorporates by reference and re-alleges each and every allegation set forth above, as though fully set forth herein.

117. As alleged herein, the Individual Defendants' wrongful conduct alleged included the failure to implement adequate internal controls to detect and prevent the breach of the Company's customers' personal and financial information. Under the Individual Defendants' supervision, Target's customers became the victims of the worst data breach in retail history.

118. The Individual Defendants caused Target to waste its valuable corporate assets by paying improper compensation and bonuses to certain of its executive officers and directors that breached their fiduciary duty.

119. As a result of the waste of corporate assets, the Individual Defendants are liable to the Company.

**COUNT IV**

**DERIVATIVELY AGAINST ALL DEFENDANTS**  
**FOR ABUSE OF CONTROL**

120. Plaintiff incorporates by reference and re-alleges each and every allegation contained above, as though fully set forth herein.

121. The Individual Defendants' misconduct alleged herein constituted an abuse of their ability to control and influence Target, for which they are legally responsible. Among the abuses of control was: (i) the Individual Defendants' failure to supervise, and to exert internal controls over, and conscious disregard of responsibilities involving maintenance of proper cyber-

security systems to protect customer personal and financial data and (ii) the Individual Defendants' reckless and/or grossly negligent failure to properly utilize the proper resources to determine whether customer data was safe within the Company's electronic systems.

122. As a direct and proximate result of defendants' abuse of control, Target has sustained significant damages.

123. As a result of the misconduct alleged herein, defendants are liable to the Company.

**PRAYER FOR RELIEF**

**WHEREFORE**, Plaintiff, demands judgment as follows:

A. Against all of the Individual Defendants and in favor of Target for the amount of damages sustained by the Company as a result of the Individual Defendants' breaches of fiduciary duty, gross mismanagement, waste of corporate assets, and abuse of control;

B. Directing Target to take all necessary actions to reform and improve its corporate governance and internal procedures to comply with applicable laws and to protect the Company and its shareholders from a repeat of the damaging events described herein;

C. Awarding to Target restitution from the Individual Defendants, and each of them, and ordering disgorgement of all profits, benefits, and other compensation obtained by the Individual Defendants;

D. Awarding the Plaintiff the costs and disbursements of this action, including reasonable attorneys' fees, accountants' and experts' fees, costs and expenses; and

E. Granting such other and further equitable relief as this Court may deem just and proper.

**JURY DEMAND**

Plaintiff demands a trial by jury.

Dated: January 29, 2014

**ANDERSON HELGEN DAVIS & NISSEN,  
P.A.**

s/Amanda R. Cefalu

Amanda R. Cefalu, Esq.  
333 South Seventh Street, Ste. 310  
Minneapolis, MN 55402  
Telephone: (612) 435-6349  
Facsimile: (612) 435-6379

**FARUQI & FARUQI, LLP**

Beth A. Keller, Esq.  
Todd H. Henderson, Esq.  
369 Lexington Avenue, 10<sup>th</sup> Floor  
New York, New York 10017  
Telephone: (212) 983-9330  
Facsimile: (212) 983-9331

-and-

**FARUQI & FARUQI, LLP**

Michael J. Hynes, Esq.  
Ligaya Hernandez, Esq.  
101 Greenwood Avenue, Suite 600  
Jenkintown, Pennsylvania 19046  
Telephone: (215) 277-5770  
Facsimile: (215) 277-5771

*Attorneys for Plaintiff*

**VERIFICATION**

I, Maureen Collier, hereby declare as follows:

I am the plaintiff in the within entitled action. I have read the Verified Shareholder Derivative Complaint. Based upon discussions with and reliance upon my counsel, and as to those facts of which I have personal knowledge, the Complaint is true and correct to the best of my knowledge, information, and belief.

I declare under penalty of perjury that the foregoing is true and correct.

Signed and Accepted:

---

Dated: January \_\_, 2014

**UNITED STATES DISTRICT COURT**

**FOR THE DISTRICT OF MINNESOTA**

THE POLICE RETIREMENT  
SYSTEM OF ST. LOUIS, Derivatively  
on Behalf of TARGET  
CORPORATION,

Plaintiff,

v.

GREGG W. STEINHAFEL, JOHN J.  
MULLIGAN, BETH M. JACOB,  
JAMES A. JOHNSON, SOLOMON D.  
TRUJILLO, ANNE M. MULCAHY,  
ROXANNE S. AUSTIN, CALVIN  
DARDEN, MARY E. MINNICK,  
DERICA W. RICE, JOHN G. STUMPF,  
DOUGLAS M. BAKER, JR.,  
HENRIQUE DE CASTRO, and  
KENNETH L. SALAZAR,

Defendants,

-and-

TARGET CORPORATION, a  
Minnesota corporation,

Nominal Defendant.

Case No. \_\_\_\_\_

**VERIFIED SHAREHOLDER  
DERIVATIVE COMPLAINT FOR  
BREACH OF FIDUCIARY DUTY  
AND WASTE OF CORPORATE  
ASSETS**

**DEMAND FOR JURY TRIAL**

### NATURE OF THE ACTION

1. This is a verified shareholder derivative action by plaintiff on behalf of nominal defendant Target Corporation ("Target" or the "Company") against certain of its officers and members of its Board of Directors (the "Board"). This action seeks to remedy defendants' violations of law, breaches of fiduciary duties, and waste of corporate assets that have caused substantial damages to the Company.

2. Target is the second largest general merchandise retailer in the United States. As part of its normal business practices, Target routinely collects its customers' personal and financial information, including credit and debit card numbers. Target assures its customers that it will protect this sensitive private information.

3. This action arises out of the Individual Defendants' (as defined herein) responsibility for the *second biggest data breach in retail history*. In violation of its express promise to do so, and contrary to reasonable customer expectations, Target failed to take reasonable steps to maintain its customers' personal and financial information in a secure manner. As a result of Target's complete and utter lack of appropriate security measures, thieves were able to steal sensitive personal and financial data from as many as *110 million* customers who shopped at Target between November 27, 2013 and December 15, 2013, the height of the 2013 holiday season. For many of these victims, identity thieves have already utilized their personal information to commit fraud and other crimes. For tens of millions of others, constant vigilance of their financial and personal records will be required to protect themselves from the threat of having their identity stolen.

4. The Individual Defendants aggravated the damage to consumers from the data breach by failing to provide adequate and prompt notice to consumers and conveying a false sense of security to affected customers. In particular, the Individual Defendants allowed Target to delay acknowledging the breach to the public until December 19, 2013, over *three weeks* after the data breach began. Worse, Target disclosed the data breach only after third-party reports already broke the news. Even then, Target concealed the full nature and scope of the data breach. In particular, Target initially reported that the data breach affected forty million people and assured those affected by the data breach that "*the issue has been identified and eliminated*," and that there was "*no indication that [personal identification number ("PIN")] numbers have been compromised*." Target further reassured worried customers that "[s]omeone cannot visit an ATM with a fraudulent debit card and withdraw cash."

5. Despite these statements, just days after Target's initial disclosure of the data breach, news outlets began reporting that encrypted PIN data had been stolen during the breach and that those codes could be used by thieves to make fraudulent withdrawals from the victims' bank accounts. Target nonetheless continued to deny that any of its customers' PIN data had been compromised.

6. Then, on December 27, 2013, Target finally admitted that customers' PIN data had been compromised in the breach. Two weeks later, on January 10, 2014, Target released another statement indicating that the breach was far more significant than the Company had been reporting. In particular, Target disclosed that an additional *seventy million* customers may have been affected by the data breach.

7. The defendants' failures to implement any internal controls at Target designed to detect and prevent such a data breach, and then timely report it, have severely damaged Target. The Company's data breach is currently under investigation by the United States Secret Service ("Secret Service"), the Department of Justice ("DOJ"), Congress, and as many as *thirty* states' Attorneys General. Moreover, there are currently no less than *sixty-seven* consumer actions filed against Target across the country. In addition, numerous class action lawsuits have been filed by financial institutions that have been forced to reissue cards and refund fraudulent purchases. These lawsuits pose the risk of hundreds of millions of dollars in damages to the Company.

8. Plaintiff now brings this litigation on behalf of Target to rectify the conduct of the individuals bearing ultimate responsibility for the corporation's misconduct—the directors and senior management.

### **JURISDICTION AND VENUE**

9. Jurisdiction is conferred by 28 U.S.C. §1332. Complete diversity among the parties exists and the amount in controversy exceeds \$75,000, exclusive of interest and costs.

10. This Court has jurisdiction over each defendant named herein because each defendant is either a corporation that conducts business in and maintains operations in this District, or is an individual who has sufficient minimum contacts with this District to render the exercise of jurisdiction by the District courts permissible under traditional notions of fair play and substantial justice.



11. Venue is proper in this Court in accordance with 28 U.S.C. §1391(a) because: (i) Target maintains its principal place of business in this District; (ii) one or more of the defendants either resides in or maintains executive offices in this District; (iii) a substantial portion of the transactions and wrongs complained of herein, including the defendants' primary participation in the wrongful acts detailed herein, and aiding and abetting and conspiracy in violation of fiduciary duties owed to Target, occurred in this District; and (iv) defendants have received substantial compensation in this District by doing business here and engaging in numerous activities that had an effect in this District.

### **THE PARTIES**

#### **Plaintiff**

12. Plaintiff, The Police Retirement System of St. Louis, was a shareholder of Target at the time of the wrongdoing complained of, has continuously been a shareholder since that time, and is a current Target shareholder. Plaintiff is a citizen of Missouri.

#### **Nominal Defendant**

13. Nominal defendant Target is a Minnesota corporation with principal executive offices located at 1000 Nicollet Mall, Minneapolis, Minnesota. Accordingly, Target is a citizen of Minnesota. Target serves guests at 1,921 stores including 1,797 in the United States and 124 in Canada. The Company operates through three reportable segments: the U.S. Retail segment, which includes all of Target's U.S. merchandising operations; the U.S. Credit Card segment, which offers credit to qualified guests through its branded proprietary credit cards; and the Canadian segment which includes costs incurred in the U.S. and Canada related to the 2013 Canadian retail market entry.

## Defendants

14. Defendant Gregg W. Steinhafel ("Steinhafel") is Target's Chief Executive Officer ("CEO") and has been since May 2008; President and has been since August 1999; Chairman of the Board and has been since February 2009; and a director and has been since 2007. Defendant Steinhafel has been employed by Target since 1979. Defendant Steinhafel knowingly, recklessly, or with gross negligence: (i) caused or allowed the Company to conceal the full scope of the data breach, which affected as many as 110 million customers; and (ii) failed to implement a system of internal controls to protect customers' personal and financial information. Target paid defendant Steinhafel the following compensation as an executive:

Fiscal Year	Salary	Stock Awards	Option Awards	Non-Equity Incentive Plan Compensation	Change in Pension Value and Nonqualified Deferred Compensation	Other Compensation	Total
2012	\$1,500,000	\$5,285,245	\$5,248,573	\$2,880,000	\$665,528	\$5,068,118	\$20,647,464

Defendant Steinhafel is a citizen of Minnesota.

15. Defendant John J. Mulligan ("Mulligan") is Target's Executive Vice President and Chief Financial Officer and has been since April 2012. Defendant Mulligan was also Target's Senior Vice President, Treasury, Accounting and Operations from February 2010 to April 2012 and Vice President, Pay and Benefits from February 2007 to February 2010. Defendant Mulligan has been employed by Target since 1979. Defendant Mulligan knowingly, recklessly, or with gross negligence: (i) caused or allowed the Company to conceal the full scope of the data breach, which affected as many as 110 million customers; and (ii) failed to implement a system of internal controls

to protect customers' personal and financial information. Target paid defendant Mulligan the following compensation as an executive:

Fiscal Year	Salary	Bonus	Stock Awards	Option Awards	Non-Equity Incentive Plan Compensation	Change in Pension Value	Other Compensation	Total
2012	\$602,404	\$371,917	\$1,395,687	\$1,340,064	\$415,250	\$35,381	\$313,505	\$4,474,208

Defendant Mulligan is a citizen of Minnesota.

16. Defendant Beth M. Jacob ("Jacob") is Target's Chief Information Officer and has been since July 2008 and Executive Vice President, Target Technology Services and has been since January 2010. Defendant Jacob was also Senior Vice President, Target Technology Services from July 2008 to January 2010 and Vice President, Guest Operations, Target Financial Services from August 2006 to July 2008. Defendant Jacob knowingly, recklessly, or with gross negligence: (i) caused or allowed the Company to conceal the full scope of the data breach, which affected as many as 110 million customers; and (ii) failed to implement a system of internal controls to protect customers' personal and financial information. Defendant Jacob is a citizen of Minnesota.

17. Defendant James A. Johnson ("Johnson") is Target's Lead Independent Director and has been since at least April 2012 and a director and has been since 1996. Defendant Johnson is also a member of Target's Corporate Responsibility Committee and has been since at least April 2012. Defendant Johnson knowingly or recklessly: (i) caused or allowed the Company to conceal the full scope of the data breach, which affected as many as 110 million customers; and (ii) failed to implement a system of

internal controls to protect customers' personal and financial information. Target paid defendant Johnson the following compensation as a director:

<b>Fiscal Year</b>	<b>Fees Paid in Cash</b>	<b>Stock Awards</b>	<b>Option Awards</b>	<b>Change in Pension Value and Nonqualified Deferred Compensation</b>	<b>Total</b>
2012	\$135,000	\$90,055	\$71,477	\$13,174	\$309,706

Defendant Johnson is a citizen of Washington, D.C.

18. Defendant Solomon D. Trujillo ("Trujillo") is a Target director and has been since 1994. Defendant Trujillo is also Chairman of Target's Corporate Responsibility Committee and has been since at least April 2012. Defendant Trujillo knowingly or recklessly: (i) caused or allowed the Company to conceal the full scope of the data breach, which affected as many as 110 million customers; and (ii) failed to implement a system of internal controls to protect customers' personal and financial information. Target paid defendant Trujillo the following compensation as a director:

<b>Fiscal Year</b>	<b>Fees Paid in Cash</b>	<b>Stock Awards</b>	<b>Option Awards</b>	<b>Change in Pension Value and Nonqualified Deferred Compensation</b>	<b>Total</b>
2012	\$105,000	\$90,055	\$71,477	\$32,165	\$298,697

Defendant Trujillo is a citizen of California.

19. Defendant Anne M. Mulcahy ("Mulcahy") is a Target director and has been since 1997. Defendant Mulcahy is also a member of Target's Audit Committee and has been since at least January 2014. Defendant Mulcahy knowingly or recklessly: (i) caused or allowed the Company to conceal the full scope of the data breach, which affected as many as 110 million customers; and (ii) failed to implement a system of internal controls

to protect customers' personal and financial information. Target paid defendant Mulcahy the following compensation as a director:

<b>Fiscal Year</b>	<b>Stock Awards</b>	<b>Total</b>
2012	\$275,003	\$275,003

Defendant Mulcahy is a citizen of Connecticut.

20. Defendant Roxanne S. Austin ("Austin") is a Target director and has been since 2002. Defendant Austin is also Chairman of Target's Audit Committee and has been since at least April 2012. Defendant Austin knowingly or recklessly: (i) caused or allowed the Company to conceal the full scope of the data breach, which affected as many as 110 million customers; and (ii) failed to implement a system of internal controls to protect customers' personal and financial information. Target paid defendant Austin the following compensation as a director:

<b>Fiscal Year</b>	<b>Fees Paid in Cash</b>	<b>Stock Awards</b>	<b>Option Awards</b>	<b>Total</b>
2012	\$120,000	\$90,055	\$71,477	\$281,532

Defendant Austin is a citizen of California.

21. Defendant Calvin Darden ("Darden") is a Target director and has been since 2003. Defendant Darden is also a member of Target's Corporate Responsibility Committee and has been since at least January 2014. Defendant Darden knowingly or recklessly: (i) caused or allowed the Company to conceal the full scope of the data breach, which affected as many as 110 million customers; and (ii) failed to implement a system of internal controls to protect customers' personal and financial information. Target paid defendant Darden the following compensation as a director:

<b>Fiscal Year</b>	<b>Fees Paid in Cash</b>	<b>Stock Awards</b>	<b>Option Awards</b>	<b>Total</b>
2012	\$90,000	\$90,055	\$71,477	\$251,532

Defendant Darden is a citizen of Georgia.

22. Defendant Mary E. Minnick ("Minnick") is a Target director and has been since 2005. Defendant Minnick is also a member of Target's Audit Committee and Corporate Responsibility Committee and has been since at least April 2012. Defendant Minnick knowingly or recklessly: (i) caused or allowed the Company to conceal the full scope of the data breach, which affected as many as 110 million customers; and (ii) failed to implement a system of internal controls to protect customers' personal and financial information. Target paid defendant Minnick the following compensation as a director:

<b>Fiscal Year</b>	<b>Stock Awards</b>	<b>Total</b>
2012	\$260,004	\$260,004

Defendant Minnick is a citizen of the United Kingdom.

23. Defendant Derica W. Rice ("Rice") is a Target director and has been since 2007. Defendant Rice is also a member of Target's Audit Committee and has been since at least April 2012. Defendant Rice knowingly or recklessly: (i) caused or allowed the Company to conceal the full scope of the data breach, which affected as many as 110 million customers; and (ii) failed to implement a system of internal controls to protect customers' personal and financial information. Target paid defendant Rice the following compensation as a director:

<b>Fiscal Year</b>	<b>Stock Awards</b>	<b>Total</b>
2012	\$260,004	\$260,004

Defendant Rice is a citizen of Indiana.

24. Defendant John G. Stumpf ("Stumpf") is a Target director and has been since 2010. Defendant Stumpf was also a member of Target's Audit Committee from at least April 2012 to March 2013. Defendant Stumpf knowingly or recklessly: (i) caused or allowed the Company to conceal the full scope of the data breach, which affected as many as 110 million customers; and (ii) failed to implement a system of internal controls to protect customers' personal and financial information. Target paid defendant Stumpf the following compensation as a director:

<b>Fiscal Year</b>	<b>Fees Paid in Cash</b>	<b>Stock Awards</b>	<b>Option Awards</b>	<b>Total</b>
2012	\$90,000	\$90,055	\$71,477	\$251,532

Defendant Stumpf is a citizen of California.

25. Defendant Douglas M. Baker, Jr. ("Baker") is a Target director and has been since March 2013. Defendant Baker was also a member of Target's Audit Committee from March 2013 to at least April 2013. Defendant Baker knowingly or recklessly: (i) caused or allowed the Company to conceal the full scope of the data breach, which affected as many as 110 million customers; and (ii) failed to implement a system of internal controls to protect customers' personal and financial information. Defendant Baker is a citizen of Minnesota.

26. Defendant Henrique De Castro ("De Castro") is a Target director and has been since March 2013. Defendant De Castro is also a member of Target's Corporate Responsibility Committee and has been since March 2013. Defendant De Castro knowingly or recklessly: (i) caused or allowed the Company to conceal the full scope of the data breach, which affected as many as 110 million customers; and (ii) failed to

implement a system of internal controls to protect customers' personal and financial information. Defendant De Castro is a citizen of California.

27. Defendant Kenneth L. Salazar ("Salazar") is a Target director and has been since July 2013. Defendant Salazar is also a member of Target's Corporate Responsibility Committee and has been since November 2013. Defendant Salazar knowingly or recklessly: (i) caused or allowed the Company to conceal the full scope of the data breach, which affected at as many as 110 million customers; and (ii) failed to implement a system of internal controls to protect customers' personal and financial information. Defendant Salazar is a citizen of Colorado.

28. The defendants identified in ¶¶14-16 are referred to herein as the "Officer Defendants." The defendants identified in ¶¶14, 17-27 are referred to herein as the "Director Defendants." The defendants identified in ¶¶19-20, 22-25 are referred to herein as the "Audit Committee Defendants." Collectively, the defendants identified in ¶¶14-27 are referred to herein as the "Individual Defendants."

## **DUTIES OF THE INDIVIDUAL DEFENDANTS**

### **Fiduciary Duties**

29. By reason of their positions as officers and directors of the Company, each of the Individual Defendants owed and owe Target and its shareholders fiduciary obligations of trust, loyalty, good faith, and due care, and were and are required to use their utmost ability to control and manage Target in a fair, just, honest, and equitable manner. The Individual Defendants were and are required to act in furtherance of the best interests of Target and not in furtherance of their personal interest or benefit.



30. To discharge their duties, the officers and directors of Target were required to exercise reasonable and prudent supervision over the management, policies, practices, and controls of the financial affairs of the Company. By virtue of such duties, the officers and directors of Target were required to, among other things:

(a) devise and maintain a system of internal controls sufficient to ensure that the Company's customers' personal and financial information is protected;

(b) ensure that the Company timely and accurately informed customers regarding any breach of their personal and financial information;

(c) conduct the affairs of the Company in an efficient, business-like manner in compliance with all applicable laws, rules, and regulations so as to make it possible to provide the highest quality performance of its business, to avoid wasting the Company's assets, and to maximize the value of the Company's stock; and

(d) remain informed as to how Target conducted its operations, and, upon receipt of notice or information of imprudent or unsound conditions or practices, make reasonable inquiry in connection therewith, and take steps to correct such conditions or practices.

#### **Breaches of Duties**

31. The conduct of the Individual Defendants complained of herein involves a knowing and culpable violation of their obligations as officers and directors of Target, the absence of good faith on their part, and a reckless disregard for their duties to the Company that the Individual Defendants were aware or reckless in not being aware posed a risk of serious injury to the Company.

32. The Individual Defendants, because of their positions of control and authority as officers and/or directors of Target, were able to and did, directly or indirectly, exercise control over the wrongful acts complained of herein. The Individual Defendants also failed to prevent the other Individual Defendants from taking such illegal actions. As a result, and in addition to the damage the Company has already incurred, Target has expended, and will continue to expend, significant sums of money.

**CONSPIRACY, AIDING AND ABETTING, AND CONCERTED ACTION**

33. In committing the wrongful acts alleged herein, the Individual Defendants have pursued, or joined in the pursuit of, a common course of conduct, and have acted in concert with and conspired with one another in furtherance of their common plan or design. In addition to the wrongful conduct herein alleged as giving rise to primary liability, the Individual Defendants further aided and abetted and/or assisted each other in breaching their respective duties.

34. The Individual Defendants engaged in a conspiracy, common enterprise, and/or common course of conduct. During this time, the Individual Defendants failed to timely and accurately inform customers regarding the full scope of the breach of their personal and financial information.

35. The purpose and effect of the Individual Defendants' conspiracy, common enterprise, and/or common course of conduct was, among other things, to disguise the Individual Defendants' violations of law, breaches of fiduciary duty, and waste of corporate assets; and to conceal adverse information concerning the Company's operations.

36. The Individual Defendants accomplished their conspiracy, common enterprise, and/or common course of conduct by allowing the Company to purposefully or recklessly conceal the scope of the data breach affecting at as many as 110 million customers. Because the actions described herein occurred under the authority of the Board, each of the Individual Defendants was a direct, necessary, and substantial participant in the conspiracy, common enterprise, and/or common course of conduct complained of herein.

37. Each of the Individual Defendants aided and abetted and rendered substantial assistance in the wrongs complained of herein. In taking such actions to substantially assist the commission of the wrongdoing complained of herein, each Individual Defendant acted with knowledge of the primary wrongdoing, substantially assisted in the accomplishment of that wrongdoing, and was aware of his or her overall contribution to and furtherance of the wrongdoing.

#### **BACKGROUND OF THE COMPANY AND ITS PRIVACY POLICY**

38. Target is the second largest general merchandise retailer in the United States. The Company operates 1,797 stores in the United States and 124 stores in Canada.

39. As stated in the Company's own "Privacy Policy," Target routinely collects personal information from its customers, including a customer's name, mailing address, e-mail address, phone number, driver's license number, and credit/debit card number. In addition, when customers use their debit cards to make a purchase at Target, they are required to enter the PIN associated with their bank account. Target promises its

customers that it will, among other things, "*maintain administrative, technical and physical safeguards to protect your personal information*." When we collect or transmit sensitive information such as a credit or debit card number, *we use industry standard methods to protect that information*."

### **The Ramifications of Failing to Keep Customers' Data Secure Are Severe**

40. Notwithstanding its promise and duties to protect its customers' sensitive personal and financial information, Target allowed the sensitive and private information of tens of millions of its customers to be stolen. Target's failure to protect its customers' sensitive personal and financial information exposes victims to identity theft. Identity theft occurs when someone wrongfully obtains another's personal information without their knowledge to commit theft or fraud.

41. Armed with a person's personal and financial information, identity thieves can encode the victim's account information onto a different card with a magnetic strip creating a counterfeit card that can be used to make fraudulent purchases. With the addition of a victim's PIN, a thief can use the counterfeit card to withdraw money from that person's bank account.

42. Identity thieves can cause further damage to their victims by using personal information to open new credit and utility accounts, receive medical treatment on their health insurance, or even obtain a driver's license. Once a person's identity has been stolen, reporting, identifying, monitoring, and repairing the victim's credit is a cumbersome, expensive, and time-consuming process. In addition to the frustration of having to identify and close affected accounts and correct information in their credit

reports, victims of identity theft often incur costs associated with defending themselves against civil litigation brought by creditors. Victims also suffer the burden of having difficulty obtaining new credit. Moreover, victims of identity theft must monitor their credit reports for future inaccuracies as fraudulent use of stolen personal information may persist for several years.

43. Annual monetary losses from identity theft total in the billions of dollars. According to The President's Identity Theft Task Force Report dated October 21, 2008, on identity theft produced in 2008:

In addition to the losses that result when identity thieves fraudulently open accounts or misuse existing accounts, ... individual victims often suffer indirect financial costs, including the costs incurred in both civil litigation initiated by creditors and in overcoming the many obstacles they face in obtaining or retaining credit. Victims of non-financial identity theft, for example, health-related or criminal record fraud, face other types of harm and frustration.

In addition to out-of-pocket expenses that can reach thousands of dollars for the victims of new account identity theft, and the emotional toll identity theft can take, some victims have to spend what can be a considerable amount of time to repair the damage caused by the identity thieves. Victims of new account identity theft, for example, must correct fraudulent information in their credit reports and monitor their reports for future inaccuracies, close existing bank accounts and open new ones, and dispute charges with individual creditors.

44. The significant impact identity theft can have on consumers, and the extreme financial ramification the failure to secure personal information can cause, has led to the enactment of numerous privacy-related laws aimed toward protecting consumer information and disclosure requirements, including, for example: (i) Gramm-Leach-Bliley Act; (ii) Fair Credit Reporting Act; (iii) Fair and Accurate Credit Transactions Act;

(iv) Federal Trade Commission Act, 15 U.S.C. §§41-58; (v) Driver's Privacy Protection Act; (vi) Health Insurance Portability and Accountability Act; (vii) The Privacy Act of 1974; (viii) Social Security Act Amendments of 1990; (ix) E-Government Act of 2002; and (x) Federal Information Security Management Act of 2002.

45. Moreover, the recent wave of cyber-attacks striking American corporations prompted warnings from federal officials, including one issued in May 2013 by the Department of Homeland Security. In particular, the warning was issued by an agency called ICS-Cert, which monitors attacks on computer systems that run industrial processes. The warning stated that the government was "highly concerned about hostility against critical infrastructure organizations."

46. In addition to the alerts from the government, Target and other retailers saw a significant uptick in malware trying to enter their systems in the year prior to the data breach.

47. The Individual Defendants were long ago notified of the risk of a potential data breach. On August 27, 2007, Dr. Neal Krawetz, a data security expert working for Hacker Factor Solutions, publicly disclosed a white paper<sup>1</sup> titled "Point-of-Sale Vulnerabilities" (the "White Paper") that warned Target about the possibility of a point-of-sale data breach. The White Paper used Target as an example of the potential

---

<sup>1</sup> A white paper is an authoritative report or guide helping readers to understand an issue, solve a problem, or make a decision. White papers are used in two main spheres: government and business-to-business marketing.

ramifications of a point-of-sale data breach at a major retailer and estimated that as many as fifty-eight million card accounts could be compromised if Target's point-of-sale system was compromised.

48. In addition to the warning in 2007, according to numerous reports, Target's computer security staff raised concerns about vulnerabilities in the Company's payment card system at least *two months* before the data breach. According to these reports, at least one analyst at the Company wanted to do a more thorough security review of its payment system—a request that was brushed off.

49. The Individual Defendants were fully aware of the ramifications of failing to keep customers' data secure and knew that the Company could be subject to costly government enforcement actions and private litigation. As stated in the risk disclosures in the Company's Annual Report on Form 10-K filed with the U.S. Securities and Exchange Commission ("SEC") on March 20, 2013:

*If we experience a significant data security breach or fail to detect and appropriately respond to a significant data security breach, we could be exposed to government enforcement actions and private litigation. In addition, our guests could lose confidence in our ability to protect their personal information, which could cause them to discontinue usage of REDcards, decline to use our pharmacy services, or stop shopping with us altogether. The loss of confidence from a significant data security breach involving team members could hurt our reputation, cause team member recruiting and retention challenges, increase our labor costs and affect how we operate our business.*

**THE INDIVIDUAL DEFENDANTS' FAILURE TO PROTECT CUSTOMERS'  
PERSONAL INFORMATION RESULTS IN RECORD-SETTING DATA  
BREACH**

50. Target's data breach compromised as many as 110 million customers' personal and financial data. Within days of the breach, millions of affected customers' financial and personal information was being sold on the black-market. Moreover, bank cards that had only been used at Target were found to have been used to make unauthorized purchases at Target stores.

51. News of the data breach first broke out on December 18, 2013, when KrebsOnSecurity.com, a website dedicated to reporting cybercrime, published an article indicating the occurrence of a massive data breach at Target stores. According to the report, Target was investigating the possible theft of millions of customer credit card and debit card records beginning November 27, 2013, and extending as far as December 15, 2013. The breach was thought to have occurred when thieves accessed the Company's customers' personal and financial data by breaking into Target's point-of-sale system.

52. According to recent reports confirmed by the Company, hackers first broke into Target's network in 2013 by stealing the login credential of a heating-and-air conditioning contractor. The contractor, Fazio Mechanical Services, has confirmed it was breached. After entering through the Company's vendor's connection, the hackers then moved laterally through Target's system, eventually accessing the system that handled payments at the Company's cash registers. There should not have been a route between a network for an outside contractor and the one for payment data.



### **Target's Initial Reports of the Data Breach Provide False Assurances to Customers**

53. Consumers were entitled to adequate and prompt notification about the data breach to help them mitigate the harm and avoid additional instances of fraud. The Individual Defendants, however, failed to take reasonable steps to have the Company notify consumers that their information had been compromised. In so doing, the Individual Defendants aggravated the damage to affected customers.

54. Only after news of the data breach spread did the Company even mention the credit card attack. On December 19, 2013, over three weeks after the data breach began, Target finally acknowledged the breach to the public. The Company issued a brief statement in which it confirmed that it had been aware of unauthorized access to certain customers' credit and debit card data at the Company's U.S. stores. According to the statement, "[a]pproximately **40 million** credit and debit card accounts may have been impacted between Nov. 27 and Dec. 15, 2013." In a separate statement issued that same day, Target conceded that customer data compromised in the data breach "included customer name, credit or debit card number, and the card's expiration date and CVV [card verification value]."

55. On December 20, 2013, in a rushed attempt to contain and minimize the perceived impact of the data breach, Target professed to "have worked swiftly to **resolve the incident**," and concluded that "there is **no indication that PIN numbers have been compromised** on affected bank issued PIN debit cards or Target debit cards." Target assured worried customers that "[s]omeone cannot visit an ATM with a fraudulent debit card and withdraw cash." That same day, Target issued a press release announcing that

*"the issue has been identified and eliminated"* and that the Company would provide free credit monitoring services to affected customers.<sup>2</sup> Moreover, in an effort to restore confidence in the Company, Target offered to extend its employees' discount of 10% to all customers who shopped in Target stores on December 21 and 22, 2013.

56. Despite Target's attempts to dispel customers' concerns, news began to emerge that credit and debit card information stolen from Target had begun to appear for sale online. According to an article by KrebsOnSecurity.com, customer account information stolen from Target was being sold on the black market "in batches of one million cards," and fraudulent purchase activity had begun being reported by issuing banks.

57. As the growing scope of the breach continued to be revealed, Target confirmed on December 23, 2013, that the Secret Service and the DOJ had decided to investigate the breach. In addition, the Attorneys General from Massachusetts, New York, Connecticut, and South Dakota also began looking into the data breach.

58. The following day, *Reuters* reported that, despite prior statements by Target to the contrary, encrypted PIN data had been stolen during the original breach, and those codes could be used by thieves to make fraudulent withdrawals from the victims' bank accounts. In response to these allegations, Target continued to deny that any of its

---

<sup>2</sup> Shortly after Target announced that it would provide free credit monitoring to customers, identity thieves began sending scam phishing e-mails to customers. These e-mails instructed the recipients to pass along their credit information so that it could be "monitored," when in fact it was being utilized for a fraudulent purpose.

customers' PIN data had been compromised. As stated in defendant Steinhafel's letter to Target's customers published shortly after the Company's initial acknowledgment of the breach:

We want you to know a few important things:

- The unauthorized access took place in U.S. Target stores between Nov. 27 and Dec. 15, 2013. Canadian stores and target.com were not affected.
- *Even if you shopped at Target during this time frame, it doesn't mean you are a victim of fraud. In fact, in other similar situations, there are typically low levels of actual fraud.*
- There is *no indication that PIN numbers have been compromised* on affected bank issued PIN debit cards or Target debit cards. *Someone cannot visit an ATM with a fraudulent debit card and withdraw cash.*
- You will not be responsible for fraudulent charges—either your bank or Target have that responsibility.

#### **The Full Scope of the Data Breach Is Revealed**

59. Then, on December 27, 2013, Target finally admitted that customers' PIN data had been compromised in the breach. Two weeks later, in yet another glaring indication that the Company had not yet "resolved" the matter, Target released a statement indicating that the breach was far more significant than the Company had been reporting. On January 10, 2014, Target disclosed that an additional **70 million** customers may have been affected by the data breach.

60. Several members of Congress have called for hearings into the Target breach, while others have asked the Federal Trade Commission to investigate the breach and take appropriate action. For example, Senator Richard Blumenthal of Connecticut

wrote to the Federal Trade Commission stating: "*If Target failed to adequately and appropriately protect its customers' data, then the breach we saw this week was not just a breach of security, it was a breach of trust.*" Similarly, Senator Al Franken of Minnesota stated that Target's security breaches "raise important questions about the responsibilities corporations have to protect consumer data and inform their customers when that data has been compromised."

61. On February 4, 2014, the Senate Judiciary Committee began to hold hearings on Target's data breach and its potential impact on the Company's customers. Defendant Mulligan appeared before the Senate Judiciary Committee and expressed that Target was "*deeply sorry*" for losing its customers' records to hackers. Defendant Mulligan stated that: "We will learn from this incident and, as a result, we hope to make Target, and our industry, more secure for customers in the future." Also at the Senate Judiciary Committee hearing, defendant Mulligan disclosed for the first time that Target found malware on twenty-five registers three days after the Company reported it had removed the threat from its system. As such, the data breach lasted until December 18, 2013, not December 15, 2013, as previously reported by the Company.

62. In addition to congressional hearings, the Company is now also facing investigations by numerous states' Attorneys General. Indeed, Lori Swanson, the Attorney General of Minnesota, stated she was joining a nationwide investigation into Target's security breach. The joint probe includes over *thirty* states' Attorneys General.

**The Individual Defendants Knew or Should Have Known that the Company's Customers Were Vulnerable to Attack Yet Failed to Implement Appropriate Security Measures**

63. Target recognizes that its customers' personal and financial information is highly sensitive and must be protected. Moreover, as discussed above, Target promises its customers that it will "maintain administrative, technical and physical safeguards to protect [customers'] information" and "use industry standard methods to protect that information." Target's Privacy Policy states:

*We maintain administrative, technical and physical safeguards to protect your personal information.* When we collect or transmit sensitive information such as a credit or debit card number, *we use industry standard methods* to protect that information.

64. The PCI Data Security Standard ("PCI") is an industry standard for large retail institutions that accept credit card and debit card transactions. The standard consists of the following twelve general requirements:

1. Install and maintain a firewall configuration to protect cardholder data;
2. Do not use vendor-supplied defaults for system passwords and other security parameters;
3. Protect stored cardholder data;
4. Encrypt transmission of cardholder data across public networks;
5. Use and regularly update anti-virus software or programs;
6. Develop and maintain secure systems and applications;

7. Restrict access to cardholder data by business need to know;
8. Assign a unique ID to each person with computer access;
9. Restrict physical access to cardholder data;
10. Track and monitor all access to network resources and cardholder data;
11. Regularly test security systems and processes; and
12. Maintain a policy that addresses information security for all personnel.

65. On December 23, 2013, *USA Today* reported that Target was likely not complying with the PCI. The article stated:

Target's massive databreach took place just a few weeks before a set of payment card industry standards – known as PCI DSS 3.0 – were scheduled to go into effect. CyberTruth asked Nick Aceto, technology director at software vendor CardConnect, to supply some clarity.

CyberTruth: What does this latest databreach tell us about the efficacy of PCI?

Aceto: We can't say definitely that this breach is a failure of Target's PCI compliance, but ***based on what Target has said, it's very hard to believe that they were even PCI 2.0 compliant at the time of the breach.***

A reason for thinking this is that the attack, involving an enormous amount of data, went on essentially unnoticed for 18 days. How were they not watching the network?

One of the PCI DSS requirements is that you monitor your logs and firewalls every day, looking for unusual activity. This monitoring involves file integrity checks and changes to critical systems files. What's more – the chapter 6 software development life cycle requires the secure distribution and verification of payment applications.

Unusual activity isn't always abnormal, but the point of PCI is to monitor and verify that all activity is normal, while not letting distractions – like

busy shopping days Black Friday and Cyber Monday, on which the breach occurred – detract from the monitoring effort.

66. The security breach could have been prevented. Security experts have indicated that Target's security system was particularly inadequate. On January 17, 2014, *The New York Times* reported:

Entering through a digital gateway, the *criminals discovered that Target's systems were astonishingly open*—lacking the virtual walls and motion detectors found in secure networks like many banks'. *Without those safeguards, the thieves moved swiftly into the company's computer servers containing Target's customer data and to the crown jewel: the in-store systems where consumers swipe their credit and debit cards and enter their PINS.*

67. The Individual Defendants knew or should have known that the Company's less than industry-standard security systems and unreasonably vulnerable technologies would render its customers an aim of attacks by third-parties. The Individual Defendants, however, failed to take corrective measures to update its systems and technologies. Among Target's deficiencies in this respect were its failure to maintain adequate backups and/or redundant systems, failure to encrypt data and establish adequate firewalls to handle a server intrusion contingency, and failure to provide prompt and adequate warnings of security breaches.

#### **DAMAGES TO TARGET**

68. As a result of the Individual Defendants' improprieties, thieves were able to steal sensitive personal and financial data from as many as 110 million customers. Target's failure to protect its customers' personal and financial information has damaged its reputation with its customer base. In addition to price, Target's current and potential

customers consider a company's ability to protect their personal and financial information when choosing where to shop. Customers are less likely to shop at stores that cannot be trusted to safeguard their sensitive private information. The impact of the breach on the Company's bottom line has already begun to be revealed. In particular, the Company has experienced "meaningfully weaker-than-expected sales since the announcement," which led the Company to cut its fourth quarter 2013 adjusted earnings per share ("EPS") of \$1.20 to \$1.30, compared to previous guidance of \$1.50 to \$1.60. The economic impact of the data breach is material to Target. The Company announced on January 22, 2014, that it was cutting health coverage for part-time workers as well as laying-off 475 workers and eliminating 700 open positions.

69. The significant nature of the impact of the data breach has caused analysts to lower their ratings and price targets for the Company. For instance, on January 21, 2014, Cowen and Co. lowered its price target for the Company from \$66 per share to \$47 per share. Indeed, Target's share price has decreased by over 11% since news of the data breach had been revealed.

70. As a direct and proximate result of the Individual Defendants' actions, Target has expended, and will continue to expend, significant sums of money. Such expenditures include, but are not limited to:

- (a) costs incurred from defending and paying any settlement in the numerous consumer class actions filed against the Company;
- (b) costs incurred from defending and paying any settlement in the numerous class actions filed by financial institutions against the Company;



(c) costs incurred from the Congressional, Attorneys General, Secret Service, and DOJ investigations into the data breach, including, but not limited to, liability for any potential fines;

(d) costs incurred from the Company's internal investigation into the data breach, including, but not limited to, expense for legal, investigative, and consulting fees;

(e) costs incurred from expenses and capital investments for remediation activities, including investing hundreds of millions of dollars in chip-enabled credit card technology;<sup>3</sup>

(f) costs incurred from notifying customers, replacing cards, sorting improper charges from legitimate charges, and reimbursing customers for improper charges;

(g) costs incurred from Target fulfilling its promise to provide free credit monitoring to victims of the data breach;

(h) loss of revenue and profit resulting from Target's offer of a 10% discount to U.S. shoppers during the last weekend before Christmas in an effort to lure customers back into its stores; and

---

<sup>3</sup> Many retailers in Europe and Canada use chip-based credit cards that are much more difficult to replicate than normal credit cards. In 2004, Target moved against chip-based credit cards out of fear that they would slow checkout speeds. Now, ten years later, Target is planning on implementing this technology to avoid further data breaches.

(i) costs incurred from compensation and benefits paid to the defendants who have breached their duties to Target.

#### **DERIVATIVE AND DEMAND FUTILITY ALLEGATIONS**

71. Plaintiff brings this action derivatively in the right and for the benefit of Target to redress injuries suffered, and to be suffered, by Target as a direct result of breaches of fiduciary duty and waste of corporate assets, as well as the aiding and abetting thereof, by the Individual Defendants. Target is named as a nominal defendant solely in a derivative capacity. This is not a collusive action to confer jurisdiction on this Court that it would not otherwise have.

72. Plaintiff will adequately and fairly represent the interests of Target in enforcing and prosecuting its rights.

73. Plaintiff was a shareholder of Target at the time of the wrongdoing complained of, has continuously been a shareholder since that time, and is a current Target shareholder.

74. The current Board of Target consists of the following twelve individuals: defendants Austin, Baker, Darden, De Castro, Johnson, Minnick, Mulcahy, Rice, Salazar, Steinhafel, Stumpf, and Trujillo. Plaintiff has not made any demand on the present Board to institute this action because such a demand would be a futile, wasteful, and useless act, as set forth below.

**Demand Is Excused Because the Director Defendants' Conduct Is Not a Valid Exercise of Business Judgment**

75. Defendants Austin, Baker, Darden, De Castro, Johnson, Minnick, Mulcahy, Rice, Salazar, Steinhafel, Stumpf, and Trujillo, constituting the Company's entire current Board, caused the Company to disseminate improper, materially false and misleading public statements concerning, among other things, the true nature and extent of the data breach. Consumers were entitled to adequate and prompt notification about the data breach to help them mitigate the harm and avoid additional instances of fraud. The Individual Defendants, however, failed to take reasonable steps to have the Company notify consumers that their information had been compromised. The Company's public disclosures concerning the data breach were improper because: (i) they were untimely and only released after third-party organizations began spreading the news; (ii) they understated the scope of the affected victims by as many as 70 million people; and (iii) they diminished the severity of the harm to customers by failing to disclose that PINs were compromised. Each member of the Board knew or should have known that the improper statements did not timely, fairly, accurately, or truthfully convey the scope of the data breach. In addition, when deciding whether to approve statements to be publicly disseminated, each member of the Board was bound by the duty of care to inform himself or herself of all reasonably-available material information. Information concerning the nature and extent of the data breach was both reasonably available and material to members of the Board. Defendants Austin, Baker, Darden, De Castro, Johnson, Minnick, Mulcahy, Rice, Salazar, Steinhafel, Stumpf, and Trujillo's conduct can in no way be

considered a valid exercise of business judgment. Accordingly, demand on the Board is excused.

**Demand Is Excused Because the Entire Board Faces a Substantial Likelihood of Liability for Their Misconduct**

76. Defendants Austin, Baker, Darden, De Castro, Johnson, Minnick, Mulcahy, Rice, Salazar, Steinhafel, Stumpf, and Trujillo, all twelve members of the current Board, are disqualified from fairly evaluating the derivative claims, let alone vigorously prosecuting them, because they are each responsible for damages suffered by Target as a result of the Company's massive data breach. The Board was responsible for ensuring that internal controls were implemented and maintained to protect the Company's customers' personal and financial information. Instead, the Board failed to implement any internal controls to detect or prevent such a data breach from occurring. Despite each Individual Defendant's responsibility for "maintain[ing] administrative, technical, and physical safeguards to protect [customers'] personal information," defendants Austin, Baker, Darden, De Castro, Johnson, Minnick, Mulcahy, Rice, Salazar, Steinhafel, Stumpf, and Trujillo took no action to ensure such protection. These defendants' complete and utter failure to establish a system of appropriate internal controls and compliance measures is a breach of their duty of loyalty. As such, the entire Board faces a substantial likelihood of liability, rendering demand upon them futile.

77. Further, defendants Austin, Baker, Darden, De Castro, Johnson, Minnick, Mulcahy, Rice, Salazar, Steinhafel, Stumpf, and Trujillo face a substantial likelihood of liability due to their failure to provide adequate and prompt notice to consumers and

because they conveyed a false sense of security to customers affected by the data breach. Defendants Austin, Baker, Darden, De Castro, Johnson, Minnick, Mulcahy, Rice, Salazar, Steinhafel, Stumpf, and Trujillo breached their duty of loyalty by causing the Company to disseminate the improper public statements discussed herein. Accordingly, all the Board members face a substantial likelihood of liability, further rendering demand upon them futile.

78. In addition to the above, defendants Austin, Minnick, Rice, and Mulcahy breached their duties as members of the Audit Committee at the time of the wrongdoing discussed herein. The Audit Committee Charter required defendants Austin, Minnick, Rice, and Mulcahy to ensure the Company's "compliance with legal and regulatory requirements," monitor the Company's internal controls, and oversee the Company's risk management. Defendants Austin, Minnick, Rice, and Mulcahy failed to fulfill these additional duties, as demonstrated by the significant nature and extent of the data breach that occurred on their watch and the inadequate notification of the data breach to customers.

79. Any suit by the current directors of Target to remedy these wrongs would expose Target to liability in the numerous pending class actions lawsuits filed on behalf of consumers and financial institutions. There are currently no less than sixty-seven consumer class actions filed against the Company as a result of the data breach. These consumer class actions allege various claims, including, but not limited to, negligence, breach of contract, and violation of state privacy laws. Moreover, Target faces several class action lawsuits on behalf of the financial institutions that lost hundreds of millions

of dollars as a result of the Company's failure to use industry-standard security methods to protect customer information. If the Board elects for the Company to press forward with its right of action against any of the members of the Board in this action, then Target's efforts would compromise its defense of the pending class actions. Accordingly, demand on the Board is excused.

80. The acts complained of constitute violations of the fiduciary duties owed by Target's officers and directors and these acts are incapable of ratification.

81. Target has been and will continue to be exposed to significant losses due to the wrongdoing complained of herein, yet the Individual Defendants and current Board have not filed any lawsuits against themselves or others who were responsible for that wrongful conduct to attempt to recover for Target any part of the damages Target suffered and will suffer thereby.

82. Plaintiff has not made any demand on the other shareholders of Target to institute this action since such demand would be a futile and useless act for at least the following reasons:

(a) Target is a publicly held company with over 632 million shares outstanding and thousands of shareholders;

(b) making demand on such a number of shareholders would be impossible for plaintiff who has no way of finding out the names, addresses, or phone numbers of shareholders; and

(c) making demand on all shareholders would force plaintiff to incur excessive expenses, assuming all shareholders could be individually identified.

## **COUNT I**

### **Against the Individual Defendants for Breach of Fiduciary Duty**

83. Plaintiff incorporates by reference and realleges each and every allegation contained above, as though fully set forth herein.

84. As alleged in detail herein, the Individual Defendants, by reason of their positions as officers and directors of Target and because of their ability to control the business and corporate affairs of Target, owed to Target fiduciary obligations of due care and loyalty, and were and are required to use their utmost ability to control and manage Target in a fair, just, honest, and equitable manner.

85. The Officer Defendants breached their duty of loyalty by knowingly, recklessly, or with gross negligence: (i) failing to implement a system of internal controls to protect customers' personal and financial information; and (ii) causing or allowing the Company to conceal the full scope of the data breach, which affected as many as 110 million customers.

86. The Director Defendants breached their duty of loyalty by knowingly or recklessly: (i) failing to implement a system of internal controls to protect customers' personal and financial information; and (ii) causing or allowing the Company to conceal the full scope of the data breach, which affected as many as 110 million customers.

87. The Audit Committee Defendants breached their fiduciary duty of loyalty by knowingly or recklessly approving the improper statements described herein, which were made during their tenure on the Audit Committee. Moreover, the Audit Committee Defendants failed to implement a system of internal controls to protect customers'

personal and financial information. The Audit Committee Defendants completely and utterly failed in their duty of oversight, as required by the Audit Committee Charter in effect at the time.

88. As a direct and proximate result of the Individual Defendants' breaches of their fiduciary obligations, Target has sustained significant damages, as alleged herein. As a result of the misconduct alleged herein, these defendants are liable to the Company.

89. Plaintiff, on behalf of Target, has no adequate remedy at law.

## **COUNT II**

### **Against all Individual Defendants for Waste of Corporate Assets**

90. Plaintiff incorporates by reference and realleges each and every allegation set forth above, as though fully set forth herein.

91. The wrongful conduct alleged included the failure to implement adequate internal controls to detect and prevent the breach of the Company's customers' personal and financial information. Under the Individual Defendants' purview, Target's customers became the victims of the second biggest data breach in retail history. The Company already incurred substantial costs in investigating the data breach and cooperating with various government investigations. In addition, the Company lost revenue and profit due to its offer of a 10% discount to U.S. shoppers during the last weekend before Christmas in an effort to lure customers back into its stores after the data breach. The Company will continue to incur substantial costs from the numerous consumer class actions filed against it.



92. Further, the Individual Defendants caused Target to waste its assets by paying improper compensation and bonuses to certain of its executive officers and directors that breached their fiduciary duty.

93. As a result of the waste of corporate assets, the Individual Defendants are liable to the Company.

94. Plaintiff, on behalf of Target, has no adequate remedy at law.

#### **PRAYER FOR RELIEF**

WHEREFORE, plaintiff, on behalf of Target, demands judgment as follows:

A. Against the Individual Defendants and in favor of the Company for the amount of damages sustained by the Company as a result of the Individual Defendants' breach of fiduciary duty, waste of corporate assets, and aiding and abetting breaches of fiduciary duties;

B. Directing Target to take all necessary actions to reform and improve its corporate governance and internal procedures to comply with applicable laws and to protect the Company and its shareholders from a repeat of the damaging events described herein, including, but not limited to, putting forward for shareholder vote, resolutions for amendments to the Company's By-Laws or Articles of Incorporation, and taking such other action as may be necessary to place before shareholders for a vote of the following Corporate Governance Policies:

1. a proposal to strengthen the Company's controls over its customers' personal and financial information;

2. a proposal to create a committee tasked with monitoring the Company's security measures;

3. a proposal to strengthen the Company's disclosure controls;

4. a proposal to strengthen the Board's supervision of operations and develop and implement procedures for greater shareholder input into the policies and guidelines of the Board; and

5. a provision to permit the shareholders of Target to nominate at least three candidates for election to the Board;

C. Awarding to Target restitution from the Individual Defendants, and each of them, and ordering disgorgement of all profits, benefits, and other compensation obtained by the Individual Defendants;

D. Awarding plaintiff the costs and disbursements of this action, including reasonable attorneys' and experts' fees, costs and expenses; and

E. Granting such other and further equitable relief as this Court may deem just and proper.

#### **JURY DEMAND**

Plaintiff demands a trial by jury.

Dated: February 27, 2014

**WALSH LAW FIRM**

/s/Christopher R. Walsh  
CHRISTOPHER R. WALSH (#199813)

Attorney at Law  
Fifth Street Towers  
100 South Fifth Street, Suite 1025  
Minneapolis, MN 55402  
Telephone: 612-767-7500  
Facsimile: 612-677-9300  
walshlawfirm@comcast.net

ROBBINS ARROYO LLP  
BRIAN J. ROBBINS  
FELIPE J. ARROYO  
SHANE P. SANDERS  
600 B Street, Suite 1900  
San Diego, CA 92101  
Telephone: (619) 525-3990  
Facsimile: (619) 525-3991  
brobbins@robbinsarroyo.com  
farroyo@robbinsarroyo.com  
ssanders@robbinsarroyo.com

Attorneys for Plaintiff

VERIFICATION


I, STEPHEN G. OLISH, hereby declare as follows:

I am the Executive Director of The Police Retirement System of St. Louis, Plaintiff in the within entitled action. I have read the Verified Shareholder Derivative Complaint for Breach of Fiduciary Duty and Waste of Corporate Assets. Based upon discussions with and reliance upon my counsel, and as to those facts of which I have personal knowledge, the Complaint is true and correct to the best of my knowledge, information, and belief.

I declare under penalty of perjury that the foregoing is true and correct.

Signed and Accepted:

Dated: 2/24/14

  
STEPHEN G. OLISH

**CIVIL COVER SHEET**

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. (SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)

**I. (a) PLAINTIFFS**

The Police Retirement System of St. Louis, Derivatively on Behalf of  
TARGET CORPORATION

(b) County of Residence of First Listed Plaintiff St. Louis City County, MO  
(EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys (Firm Name, Address, and Telephone Number)

Christopher R. Walsh (#199813), Walsh Law Firm, Fifth Street Towers,  
100 South Fifth Street, Suite 1025, Minneapolis, MN 55402; Telephone  
(612) 767-7500

**DEFENDANTS**

GREGG W. STEINHAFEL, JOHN J. MULLIGAN, BETH M. JACOB,  
JAMES A. JOHNSON, SOLOMON D. TRUJILLO, ANNE M.  
MULCAHY, ROXANNE S. AUSTIN, CALVIN DARDEN, et al.

County of Residence of First Listed Defendant Hennepin County, MN  
(IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF  
THE TRACT OF LAND INVOLVED.

Attorneys (If Known)

**II. BASIS OF JURISDICTION** (Place an "X" in One Box Only)

- ☐ 1 U.S. Government Plaintiff
- ☐ 3 Federal Question (U.S. Government Not a Party)
- ☐ 2 U.S. Government Defendant
- ☒ 4 Diversity (Indicate Citizenship of Parties in Item III)

**III. CITIZENSHIP OF PRINCIPAL PARTIES** (Place an "X" in One Box for Plaintiff and One Box for Defendant)

- |   | PTF                                   | DEF                        |   | PTF                        | DEF                                   |
|---|---------------------------------------|----------------------------|---|----------------------------|---------------------------------------|
| Citizen of This State                   | <input type="checkbox"/> 1            | <input type="checkbox"/> 1 | Incorporated or Principal Place of Business In This State     | <input type="checkbox"/> 4 | <input checked="" type="checkbox"/> 4 |
| Citizen of Another State                | <input checked="" type="checkbox"/> 2 | <input type="checkbox"/> 2 | Incorporated and Principal Place of Business In Another State | <input type="checkbox"/> 5 | <input type="checkbox"/> 5            |
| Citizen or Subject of a Foreign Country | <input type="checkbox"/> 3            | <input type="checkbox"/> 3 | Foreign Nation  | <input type="checkbox"/> 6 | <input type="checkbox"/> 6            |

**IV. NATURE OF SUIT** (Place an "X" in One Box Only)

CONTRACT	TORTS	FORFEITURE/PENALTY	BANKRUPTCY	OTHER STATUTES	
<input type="checkbox"/> 110 Insurance <input type="checkbox"/> 120 Marine <input type="checkbox"/> 130 Miller Act <input type="checkbox"/> 140 Negotiable Instrument <input type="checkbox"/> 150 Recovery of Overpayment & Enforcement of Judgment <input type="checkbox"/> 151 Medicare Act <input type="checkbox"/> 152 Recovery of Defaulted Student Loans (Excludes Veterans) <input type="checkbox"/> 153 Recovery of Overpayment of Veteran's Benefits <input checked="" type="checkbox"/> 160 Stockholders' Suits <input type="checkbox"/> 190 Other Contract <input type="checkbox"/> 195 Contract Product Liability <input type="checkbox"/> 196 Franchise	<b>PERSONAL INJURY</b> <input type="checkbox"/> 310 Airplane <input type="checkbox"/> 315 Airplane Product Liability <input type="checkbox"/> 320 Assault, Libel & Slander <input type="checkbox"/> 330 Federal Employers' Liability <input type="checkbox"/> 340 Marine <input type="checkbox"/> 345 Marine Product Liability <input type="checkbox"/> 350 Motor Vehicle <input type="checkbox"/> 355 Motor Vehicle Product Liability <input type="checkbox"/> 360 Other Personal Injury <input type="checkbox"/> 362 Personal Injury - Medical Malpractice	<b>PERSONAL INJURY</b> <input type="checkbox"/> 365 Personal Injury - Product Liability <input type="checkbox"/> 367 Health Care/Pharmaceutical Personal Injury Product Liability <input type="checkbox"/> 368 Asbestos Personal Injury Product Liability <b>PERSONAL PROPERTY</b> <input type="checkbox"/> 370 Other Fraud <input type="checkbox"/> 371 Truth in Lending <input type="checkbox"/> 380 Other Personal Property Damage <input type="checkbox"/> 385 Property Damage Product Liability	<input type="checkbox"/> 625 Drug Related Seizure of Property 21 USC 881 <input type="checkbox"/> 690 Other <b>LABOR</b> <input type="checkbox"/> 710 Fair Labor Standards Act <input type="checkbox"/> 720 Labor/Management Relations <input type="checkbox"/> 740 Railway Labor Act <input type="checkbox"/> 751 Family and Medical Leave Act <input type="checkbox"/> 790 Other Labor Litigation <input type="checkbox"/> 791 Employee Retirement Income Security Act <b>IMMIGRATION</b> <input type="checkbox"/> 462 Naturalization Application <input type="checkbox"/> 465 Other Immigration Actions	<input type="checkbox"/> 422 Appeal 28 USC 158 <input type="checkbox"/> 423 Withdrawal 28 USC 157 <b>PROPERTY RIGHTS</b> <input type="checkbox"/> 820 Copyrights <input type="checkbox"/> 830 Patent <input type="checkbox"/> 840 Trademark <b>SOCIAL SECURITY</b> <input type="checkbox"/> 861 HIA (1395ff) <input type="checkbox"/> 862 Black Lung (923) <input type="checkbox"/> 863 DIWC/DIWW (405(g)) <input type="checkbox"/> 864 SSID Title XVI <input type="checkbox"/> 865 RSI (405(g)) <b>FEDERAL TAX SUITS</b> <input type="checkbox"/> 870 Taxes (U.S. Plaintiff or Defendant) <input type="checkbox"/> 871 IRS—Third Party 26 USC 7609	<input type="checkbox"/> 375 False Claims Act <input type="checkbox"/> 400 State Reapportionment <input type="checkbox"/> 410 Antitrust <input type="checkbox"/> 430 Banks and Banking <input type="checkbox"/> 450 Commerce <input type="checkbox"/> 460 Deportation <input type="checkbox"/> 470 Racketeer Influenced and Corrupt Organizations <input type="checkbox"/> 480 Consumer Credit <input type="checkbox"/> 490 Cable/Sat TV <input type="checkbox"/> 850 Securities/Commodities/Exchange <input type="checkbox"/> 890 Other Statutory Actions <input type="checkbox"/> 891 Agricultural Acts <input type="checkbox"/> 893 Environmental Matters <input type="checkbox"/> 895 Freedom of Information Act <input type="checkbox"/> 896 Arbitration <input type="checkbox"/> 899 Administrative Procedure Act/Review or Appeal of Agency Decision <input type="checkbox"/> 950 Constitutionality of State Statutes
<b>REAL PROPERTY</b> <input type="checkbox"/> 210 Land Condemnation <input type="checkbox"/> 220 Foreclosure <input type="checkbox"/> 230 Rent Lease & Ejectment <input type="checkbox"/> 240 Torts to Land <input type="checkbox"/> 245 Tort Product Liability <input type="checkbox"/> 290 All Other Real Property	<b>CIVIL RIGHTS</b> <input type="checkbox"/> 440 Other Civil Rights <input type="checkbox"/> 441 Voting <input type="checkbox"/> 442 Employment <input type="checkbox"/> 443 Housing/Accommodations <input type="checkbox"/> 445 Amer. w/Disabilities - Employment <input type="checkbox"/> 446 Amer. w/Disabilities - Other <input type="checkbox"/> 448 Education	<b>PRISONER PETITIONS</b> <b>Habeas Corpus:</b> <input type="checkbox"/> 463 Alien Detainee <input type="checkbox"/> 510 Motions to Vacate Sentence <input type="checkbox"/> 530 General <input type="checkbox"/> 535 Death Penalty <b>Other:</b> <input type="checkbox"/> 540 Mandamus & Other <input type="checkbox"/> 550 Civil Rights <input type="checkbox"/> 555 Prison Condition <input type="checkbox"/> 560 Civil Detainee - Conditions of Confinement			

**V. ORIGIN** (Place an "X" in One Box Only)

- ☒ 1 Original Proceeding
- ☐ 2 Removed from State Court
- ☐ 3 Remanded from Appellate Court
- ☐ 4 Reinstated or Reopened
- ☐ 5 Transferred from Another District (specify)
- ☐ 6 Multidistrict Litigation

**VI. CAUSE OF ACTION**

Cite the U.S. Civil Statute under which you are filing (Do not cite jurisdictional statutes unless diversity):  
28 U.S.C. §1332

Brief description of cause:

Shareholder Derivative Action for Breach of Fiduciary Duty and Waste of Corporate Assets

**VII. REQUESTED IN COMPLAINT:**

☐ CHECK IF THIS IS A CLASS ACTION UNDER RULE 23, F.R.Cv.P.

DEMAND \$

CHECK YES only if demanded in complaint:

JURY DEMAND: ☒ Yes ☐ No

**VIII. RELATED CASE(S) IF ANY**

(See instructions):

JUDGE Susan Richard Nelson

DOCKET NUMBER 0:14-cv-02203-SRN-JSM

DATE

02/27/2014

SIGNATURE OF ATTORNEY OF RECORD

/s/ Christopher R. Walsh

FOR OFFICE USE ONLY

RECEIPT # \_\_\_\_\_ AMOUNT \_\_\_\_\_ APPLYING IFP \_\_\_\_\_ JUDGE \_\_\_\_\_ MAG. JUDGE \_\_\_\_\_

**INSTRUCTIONS FOR ATTORNEYS COMPLETING CIVIL COVER SHEET FORM JS 44****Authority For Civil Cover Sheet**

The JS 44 civil cover sheet and the information contained herein neither replaces nor supplements the filings and service of pleading or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. Consequently, a civil cover sheet is submitted to the Clerk of Court for each civil complaint filed. The attorney filing a case should complete the form as follows:

- I.(a) Plaintiffs-Defendants.** Enter names (last, first, middle initial) of plaintiff and defendant. If the plaintiff or defendant is a government agency, use only the full name or standard abbreviations. If the plaintiff or defendant is an official within a government agency, identify first the agency and then the official, giving both name and title.
  - (b) County of Residence.** For each civil case filed, except U.S. plaintiff cases, enter the name of the county where the first listed plaintiff resides at the time of filing. In U.S. plaintiff cases, enter the name of the county in which the first listed defendant resides at the time of filing. (NOTE: In land condemnation cases, the county of residence of the "defendant" is the location of the tract of land involved.)
  - (c) Attorneys.** Enter the firm name, address, telephone number, and attorney of record. If there are several attorneys, list them on an attachment, noting in this section "(see attachment)".
- II. Jurisdiction.** The basis of jurisdiction is set forth under Rule 8(a), F.R.Cv.P., which requires that jurisdictions be shown in pleadings. Place an "X" in one of the boxes. If there is more than one basis of jurisdiction, precedence is given in the order shown below.
- United States plaintiff. (1) Jurisdiction based on 28 U.S.C. 1345 and 1348. Suits by agencies and officers of the United States are included here.
- United States defendant. (2) When the plaintiff is suing the United States, its officers or agencies, place an "X" in this box.
- Federal question. (3) This refers to suits under 28 U.S.C. 1331, where jurisdiction arises under the Constitution of the United States, an amendment to the Constitution, an act of Congress or a treaty of the United States. In cases where the U.S. is a party, the U.S. plaintiff or defendant code takes precedence, and box 1 or 2 should be marked.
- Diversity of citizenship. (4) This refers to suits under 28 U.S.C. 1332, where parties are citizens of different states. When Box 4 is checked, the citizenship of the different parties must be checked. (See Section III below; **NOTE: federal question actions take precedence over diversity cases.**)
- III. Residence (citizenship) of Principal Parties.** This section of the JS 44 is to be completed if diversity of citizenship was indicated above. Mark this section for each principal party.
- IV. Nature of Suit.** Place an "X" in the appropriate box. If the nature of suit cannot be determined, be sure the cause of action, in Section VI below, is sufficient to enable the deputy clerk or the statistical clerk(s) in the Administrative Office to determine the nature of suit. If the cause fits more than one nature of suit, select the most definitive.
- V. Origin.** Place an "X" in one of the six boxes.
- Original Proceedings. (1) Cases which originate in the United States district courts.
- Removed from State Court. (2) Proceedings initiated in state courts may be removed to the district courts under Title 28 U.S.C., Section 1441. When the petition for removal is granted, check this box.
- Remanded from Appellate Court. (3) Check this box for cases remanded to the district court for further action. Use the date of remand as the filing date.
- Reinstated or Reopened. (4) Check this box for cases reinstated or reopened in the district court. Use the reopening date as the filing date.
- Transferred from Another District. (5) For cases transferred under Title 28 U.S.C. Section 1404(a). Do not use this for within district transfers or multidistrict litigation transfers.
- Multidistrict Litigation. (6) Check this box when a multidistrict case is transferred into the district under authority of Title 28 U.S.C. Section 1407. When this box is checked, do not check (5) above.
- VI. Cause of Action.** Report the civil statute directly related to the cause of action and give a brief description of the cause. **Do not cite jurisdictional statutes unless diversity.** Example: U.S. Civil Statute: 47 USC 553 Brief Description: Unauthorized reception of cable service
- VII. Requested in Complaint.** Class Action. Place an "X" in this box if you are filing a class action under Rule 23, F.R.Cv.P.
- Demand. In this space enter the actual dollar amount being demanded or indicate other demand, such as a preliminary injunction.
- Jury Demand. Check the appropriate box to indicate whether or not a jury is being demanded.
- VIII. Related Cases.** This section of the JS 44 is used to reference related pending cases, if any. If there are related pending cases, insert the docket numbers and the corresponding judge names for such cases.

**Date and Attorney Signature.** Date and sign the civil cover sheet.



### NATURE OF THE ACTION

"Some organizations will be a target regardless of what they do, but most become a target *because* of what they do (or don't do)."

-Verizon 2012 Data Breach Investigations Report.

1. Plaintiffs commenced this shareholder derivative case after the actions and conscious inaction of top-level executives and directors of Target Corporation ("Target" or the "Company") resulted in one of the largest data breaches in U.S. history. Plaintiffs assert claims derivatively on behalf of Target for breach of fiduciary duty and waste of corporate assets against certain current and former Company officers and members of Target's Board of Directors (the "Board").

2. Target, one of the largest retailers in the U.S., has an extensive computer network that was first hacked between 2005 and 2007. Target's Board and top officers knew long before (and certainly after) those attacks that the Company's point-of-sale ("POS") machines were vulnerable, but nonetheless decided against updating POS systems in the Company's U.S. stores. The Company bought a new state-of-the-art program to protect its servers, but did not take the time and effort to develop data security controls and implement industry best practices. Instead, the Board and certain executives utterly failed to implement and oversee the people, policies, and procedures necessary to successfully run the program.

3. In addition to the prior attacks at Target (and similar attacks at other companies), defendants ignored the chorus of warnings about data security risks in recent years, and failed to take steps to prevent the now-infamous 2013 holiday season data



breach at Target that caused such significant harm to the Company and its shareholders. For example, many of the defendants learned of the risk of a potential security breach as early as 2007, when a data security expert publicly disclosed a White Paper<sup>1</sup> that warned Target about the possibility of a POS security breach and estimated that as many as fifty-eight million card accounts could be compromised if Target's POS system was hacked. Then, in 2011, Target became the subject of a massive online security breach involving other large U.S. companies that exposed Target customers' names and e-mail addresses. At the time, security experts publicly commented that the breach put Target customers at risk by exposing them to phishing e-mails seeking credit card and other financial information. Similarly, the Board failed to update Target's corporate governance or risk management practices despite widespread recognition of the potential harm from a data breach. Despite these and other explicit warnings, the defendants failed to ensure that Target complied with even the most basic and fundamental industry standards for protecting consumer information that are common for large retail institutions accepting credit card and debit card transactions.

4. As a result of the defendants' failures to ensure the implementation and oversight of an adequate internal control system concerning data security risks, shortly before the 2013 holiday season, hackers gained access to Target's servers via an

---

<sup>1</sup> A White Paper is an authoritative report or guide helping readers to understand an issue, solve a problem, or make a decision. White Papers are used in two main spheres: government and business-to-business marketing.

unsecured third- party connection—an unlocked backdoor. This backdoor entry was particularly vulnerable because Target did not follow standard information technology ("IT") security practices and published extensive information about its computer system on the Internet. Once inside, the hackers were able to migrate across the system because firewalls and other common protective measures were not in place. The hackers installed malicious software that recorded the personal and financial information of Target shoppers and saved it in a location hidden within Target's network. When Target's new security program discovered the issue, it alerted Target's security team in India, who elevated the threat to Target's higher-level security operations center based out of Target's Minnesota headquarters. In response, Target's security personnel did nothing. They stood idly by while hackers stole 110 million customers' personal and financial records, affecting one out of three Americans. Indeed, a *Bloomberg* report has confirmed—based on interviews with at least ten former Target employees familiar with the Company's data security operation, including some with specific knowledge of the breach and its aftermath at the Company—that even though management was alerted to the risks Target's lax oversight posed to the Company in the weeks leading up to the breach, they stood idly by as forty million customer credit card numbers, and seventy million customer addresses, phone numbers, and other pieces of personal information, gushed out of its mainframes. Target's Board members (and the other defendants) were not even aware of the attack until they were informed by the U.S. Secret Service.

5. In addition to their egregious oversight lapses on the front end, the defendants failed to take reasonable steps to ensure that the Company timely notified

consumers that its information security system had been breached, putting customers at additional risk and causing further damage to Target. The Company's tardy disclosures significantly downplayed the nature and extent of the breach, such as denying that that Personal Identification Numbers ("PINs") had been compromised. Mere days after those statements, *Reuters* reported that despite prior statements by Target to the contrary, encrypted PIN data had been stolen during the original breach, and those codes could be used by thieves to make fraudulent withdrawals from the victims' bank accounts. And just a week after Target's baseless public assurances, the Company was forced to admit that it had not yet "resolved" the matter, admitting that the breach was far more significant than the Company had been reporting and disclosing that hackers had also stolen the personal information of an additional seventy million customers.

6. Plaintiffs now bring suit derivatively on Target's behalf to remedy the defendants' failure to act to protect the Company from known vulnerabilities in its network. The defendants breached their fiduciary duties of loyalty, good faith, and due care by knowingly and/or in conscious disregard of their duties: (i) failing to implement a system of internal controls to protect customers' personal and financial information; and (ii) failing to oversee and monitor the Company's internal control system, resulting in inadequate internal controls that did not protect customers' personal and financial information. For example, the defendants failed to ensure, among other things, that the Company had formal data security risk management guidelines, policies, and procedures in place, that individuals with the requisite expertise and understanding of data security issues were appointed to appropriate positions, and that a Chief Information Security

Officer ("CISO") with the ability to explain the risks and vulnerabilities to the defendants was in place. Because of this, Target was a "target," and hackers hit the bull's-eye. The defendants also breached their fiduciary duties by causing and/or consciously permitting the Company to conceal the full scope of the data breach and to provide inaccurate, untimely information about it.

7. The defendants' failure to protect its customers' personal and financial information has damaged Target's reputation with its customer base, and the impact of the breach on the Company's bottom line has been substantial. Target also has already incurred substantial costs, and will be forced to incur substantial additional costs, in connection with the following, among other things: (i) lost revenue and profits resulting from diminished consumer confidence in Target's information security and the costs of restitution to customers affected by the security breach; (ii) various investigations into the breach, including, but not limited to, expenses for legal, investigative, and consulting fees, and liability for potential resulting fines and penalties; (iii) increased cost of capital due to credit rating downgrades resulting from the breach; (iv) defending and paying any settlement or judgment in the class actions brought by financial institutions alleging that they sustained millions of dollars of damages due to the breach associated with the costs of notifying their customers regarding replacing cards, sorting improper charges from legitimate charges, and reimbursing customers for improper charges; (v) defending and paying any settlement or judgment in the class actions brought by Target consumers; and (vi) paying compensation and benefits to the defendants who have breached their duties to the Company. In addition to seeking monetary relief for these damages suffered by

Target, plaintiffs also seek improvements to the Company's corporate governance structure, which will help restore consumer confidence in its ability to protect customers' sensitive personal and financial information.

### **JURISDICTION AND VENUE**

8. Jurisdiction is conferred by 28 U.S.C. §1332. Complete diversity among the parties exists and the amount in controversy exceeds \$75,000, exclusive of interest and costs.

9. This Court has jurisdiction over each defendant named herein because each defendant is either a corporation that conducts business in and maintains operations in this District, or is an individual who has sufficient minimum contacts with this District to render the exercise of jurisdiction by the District courts permissible under traditional notions of fair play and substantial justice.

10. Venue is proper in this Court in accordance with 28 U.S.C. §1391(a) because: (i) Target maintains its principal place of business in this District; (ii) one or more of the defendants either resides in or maintains executive offices in this District; (iii) a substantial portion of the transactions and wrongs complained of herein, including the defendants' primary participation in the wrongful acts detailed herein, and aiding and abetting and conspiracy in violation of fiduciary duties owed to Target, occurred in this District; and (iv) defendants have received substantial compensation in this District by doing business here and engaging in numerous activities that had an effect in this District.

## **THE PARTIES**

### **Plaintiffs**

11. Plaintiff Mary Davis has held shares of Target stock continuously since at least January 20, 2009, and is a current Target shareholder. Plaintiff Davis is a citizen of New York.

12. Plaintiff Maureen Collier has held shares of Target stock continuously since at least December 14, 2011, and is a current Target shareholder. Plaintiff Collier is a citizen of Florida.

13. Plaintiff The Police Retirement System of St. Louis has held shares of Target stock continuously since at least July 31, 2011, and is a current Target shareholder. Plaintiff The Police Retirement System of St. Louis is a citizen of Missouri.

### **Nominal Defendant**

14. Nominal defendant Target is a Minnesota corporation with principal executive offices located at 1000 Nicollet Mall, Minneapolis, Minnesota. Accordingly, Target is a citizen of Minnesota. Target operates 1,921 retail stores, including 1,797 in the United States and 124 in Canada. The Company operates through three reportable segments: the U.S. Retail segment, which includes all of Target's U.S. merchandising operations; the U.S. Credit Card segment, which offers credit to qualified customers through its branded proprietary credit cards; and the Canadian segment, which includes costs incurred in the U.S. and Canada related to the 2013 Canadian retail market entry.

## Defendants

15. Defendant Gregg W. Steinhafel ("Steinhafel") was Target's Chief Executive Officer ("CEO") from May 2008 to May 2014, when he "resigned" after a precipitous drop in the value of Target shares following the data breach; President from August 1999 to May 2014; Chairman of the Board from February 2009 to May 2014; and a director from 2007 to May 2014. Despite defendant Steinhafel's responsibility for much of the wrongdoing alleged herein, the Board has permitted him to remain employed by Target in an "advisory capacity," earning roughly the same salary as he did when he was the Company's CEO, and to receive a handsome severance package worth at least \$7 million when his employment at the Company is finally terminated. Defendant Steinhafel has been employed by Target since 1979. Defendant Steinhafel knowingly and/or in conscious disregard of his duties: (i) failed to implement a system of internal controls to protect customers' personal and financial information; (ii) failed to oversee and monitor the Company's internal controls system, resulting in inadequate internal controls that failed to protect customers' personal and financial information; and (iii) caused and/or consciously permitted the Company to conceal the full scope of the data breach and to provide inaccurate, untimely information about it. Target paid defendant Steinhafel the following compensation:

Fiscal Year	Salary	Stock Awards	Option Awards	Non-Equity Incentive Plan Compensation	Change in Pension Value and Nonqualified Deferred Compensation	Other Compensation	Total
2013	\$1,500,000	\$10,224,120	-	-	\$720,219	\$508,875	\$12,953,214
2012	\$1,500,000	\$5,285,245	\$5,248,573	\$2,880,000	\$665,528	\$5,068,118	\$20,647,464

Defendant Steinhafel is a citizen of Minnesota.

16. Defendant Beth M. Jacob ("Jacob") was Target's Chief Information Officer ("CIO") from July 2008 to March 2014, and Executive Vice President, Target Technology Services from January 2010 to March 2014, when she "resigned" after presiding over one of the largest information thefts in history. Defendant Jacob was also Senior Vice President, Target Technology Services from July 2008 to January 2010, and Vice President, Guest Operations, Target Financial Services from August 2006 to July 2008. Defendant Jacob knowingly, and/or in conscious disregard of her duties: (i) failed to implement a system of internal controls to protect customers' personal and financial information; (ii) failed to oversee and monitor the Company's internal controls system, resulting in inadequate internal controls that failed to protect customers' personal and financial information; and (iii) caused and/or consciously permitted the Company to conceal the full scope of the data breach and to provide inaccurate, untimely information about it. Defendant Jacob is a citizen of Minnesota.

17. Defendant John Mulligan ("Mulligan") is Target's Executive Vice President and Chief Financial Officer ("CFO") and has been since April 2012 and Interim President and CEO and has been since May 2014. Defendant Mulligan was also Target's Senior Vice President, Treasury, Accounting and Operations from February 2010 to April 2012 and Vice President, Pay and Benefits from February 2007 to February 2010. Defendant Mulligan has worked at Target since 1996. Defendant Mulligan knowingly, and/or in conscious disregard of his duties: (i) failed to implement a system of internal controls to protect customers' personal and financial information; (ii) failed to oversee and monitor the Company's internal controls system, resulting in inadequate internal controls that



failed to protect customers' personal and financial information; and (iii) caused and/or consciously permitted the Company to conceal the full scope of the data breach and to provide inaccurate, untimely information about it. Target paid defendant Mulligan the following compensation:

Fiscal Year	Salary	Stock Awards	Option Awards	Non-Equity Incentive Plan Compensation	Change in Pension Value	Other Compensation	Total
2013	\$700,000	\$3,505,105	-	-	\$5,465	\$273,286	\$4,633,856
2012	\$602,404	\$1,395,687	\$1,340,064	\$415,250	\$35,381	\$313,505	\$4,474,208

Defendant Mulligan is a citizen of Minnesota.

18. Defendant James A. Johnson ("Johnson") is Target's Lead Independent Director and has been since at least April 2012 and a director and has been since 1996. Defendant Johnson is also a member of Target's Corporate Responsibility Committee and has been since at least April 2012. Defendant Johnson knowingly and/or in conscious disregard of his duties: (i) failed to implement a system of internal controls to protect customers' personal and financial information; (ii) failed to oversee and monitor the Company's internal controls system, resulting in inadequate internal controls that failed to protect customers' personal and financial information; and (iii) caused and/or consciously permitted the Company to conceal the full scope of the data breach and to provide inaccurate, untimely information about it. Target paid defendant Johnson the following compensation:

Fiscal Year	Fees Paid in Cash	Stock Awards	Option Awards	Change in Pension Value and Nonqualified Deferred Compensation	Total
2013	\$135,000	\$170,013	-	\$17,037	\$322,050
2012	\$135,000	\$90,055	\$71,477	\$13,174	\$309,706

Defendant Johnson is a citizen of Washington, D.C.

19. Defendant Anne M. Mulcahy ("Mulcahy") is a Target director and has been since 1997. Defendant Mulcahy is also a member of Target's Audit Committee and has been since at least January 2014. Defendant Mulcahy knowingly and/or in conscious disregard of her duties: (i) failed to implement a system of internal controls to protect customers' personal and financial information; (ii) failed to oversee and monitor the Company's internal controls system, resulting in inadequate internal controls that failed to protect customers' personal and financial information; and (iii) caused and/or consciously permitted the Company to conceal the full scope of the data breach and to provide inaccurate, untimely information about it. Target paid defendant Mulcahy the following compensation:

<b>Fiscal Year</b>	<b>Stock Awards</b>	<b>Total</b>
2013	\$170,013	\$170,013
2012	\$275,003	\$275,003

Defendant Mulcahy is a citizen of Connecticut.

20. Defendant Roxanne S. Austin ("Austin") is Target's Interim Chair of the Board and has been since May 2014 and a Target director and has been since 2002. Defendant Austin is also Chairman of Target's Audit Committee and has been since at least April 2012. Defendant Austin knowingly and/or in conscious disregard of her duties: (i) failed to implement a system of internal controls to protect customers' personal and financial information; (ii) failed to oversee and monitor the Company's internal controls system, resulting in inadequate internal controls that failed to protect customers'

personal and financial information; and (iii) caused and/or consciously permitted the Company to conceal the full scope of the data breach and to provide inaccurate, untimely information about it. Target paid defendant Austin the following compensation:

<b>Fiscal Year</b>	<b>Fees Paid in Cash</b>	<b>Stock Awards</b>	<b>Option Awards</b>	<b>Total</b>
2013	\$120,000	\$170,013		\$290,013
2012	\$120,000	\$90,055	\$71,477	\$281,532

Defendant Austin is a citizen of California.

21. Defendant Calvin Darden ("Darden") is a Target director and has been since 2003. Defendant Darden is also a member of Target's Corporate Responsibility Committee and has been since at least January 2014. Defendant Darden knowingly and/or in conscious disregard of his duties: (i) failed to implement a system of internal controls to protect customers' personal and financial information; (ii) failed to oversee and monitor the Company's internal controls system, resulting in inadequate internal controls that failed to protect customers' personal and financial information; and (iii) caused and/or consciously permitted the Company to conceal the full scope of the data breach and to provide inaccurate, untimely information about it. Target paid defendant Darden the following compensation:

<b>Fiscal Year</b>	<b>Fees Paid in Cash</b>	<b>Stock Awards</b>	<b>Option Awards</b>	<b>Total</b>
2013	\$90,000	\$170,013	-	\$260,013
2012	\$90,000	\$90,055	\$71,477	\$251,532

Defendant Darden is a citizen of Georgia.

22. Defendant Mary E. Minnick ("Minnick") is a Target director and has been since 2005. Defendant Minnick is also a member of Target's Audit Committee and Corporate Responsibility Committee and has been since at least April 2012. Defendant Minnick knowingly and/or in conscious disregard of her duties: (i) failed to implement a system of internal controls to protect customers' personal and financial information; (ii) failed to oversee and monitor the Company's internal controls system, resulting in inadequate internal controls that failed to protect customers' personal and financial information; and (iii) caused and/or consciously permitted the Company to conceal the full scope of the data breach and to provide inaccurate, untimely information about it. Target paid defendant Minnick the following compensation:

<b>Fiscal Year</b>	<b>Stock Awards</b>	<b>Total</b>
2013	\$260,061	\$260,061
2012	\$260,004	\$260,004

Defendant Minnick is a citizen of the United Kingdom.

23. Defendant Derica W. Rice ("Rice") is a Target director and has been since 2007. Defendant Rice is also a member of Target's Audit Committee and has been since at least April 2012. Defendant Rice knowingly and/or in conscious disregard of her duties: (i) failed to implement a system of internal controls to protect customers' personal and financial information; (ii) failed to oversee and monitor the Company's internal controls system, resulting in inadequate internal controls that failed to protect customers' personal and financial information; and (iii) caused and/or consciously permitted the

Company to conceal the full scope of the data breach and to provide inaccurate, untimely information about it. Target paid defendant Rice the following compensation:

<b>Fiscal Year</b>	<b>Fees Paid in Cash</b>	<b>Stock Awards</b>	<b>Total</b>
2013	\$12,500	\$275,027	\$287,527
2012	-	\$260,004	\$260,004

Defendant Rice is a citizen of Indiana.

24. Defendant John G. Stumpf ("Stumpf") is a Target director and has been since 2010. Defendant Stumpf was also a member of Target's Audit Committee from at least April 2012 to March 2013. Defendant Stumpf knowingly and/or in conscious disregard of his duties: (i) failed to implement a system of internal controls to protect customers' personal and financial information; (ii) failed to oversee and monitor the Company's internal controls system, resulting in inadequate internal controls that failed to protect customers' personal and financial information; and (iii) caused and/or consciously permitted the Company to conceal the full scope of the data breach and to provide inaccurate, untimely information about it. As a director Target paid defendant Stumpf the following compensation:

<b>Fiscal Year</b>	<b>Fees Paid in Cash</b>	<b>Stock Awards</b>	<b>Option Awards</b>	<b>Total</b>
2013	\$90,000	\$170,013	-	\$260,013
2012	\$90,000	\$90,055	\$71,477	\$251,532

Defendant Stumpf is a citizen of California.

25. Defendant Douglas M. Baker, Jr. ("Baker") is a Target director and has been since March 2013. Defendant Baker was also a member of Target's Audit

Committee from March 2013 to at least April 2013. Defendant Baker knowingly and/or in conscious disregard of his duties: (i) failed to implement a system of internal controls to protect customers' personal and financial information; (ii) failed to oversee and monitor the Company's internal controls system, resulting in inadequate internal controls that failed to protect customers' personal and financial information; and (iii) caused and/or consciously permitted the Company to conceal the full scope of the data breach and to provide inaccurate, untimely information about it. Defendant Baker is a citizen of Minnesota.

26. Defendant Henrique De Castro ("De Castro") is a Target director and has been since March 2013. Defendant De Castro is also a member of Target's Corporate Responsibility Committee and has been since March 2013. Defendant De Castro and/or in conscious disregard of his duties: (i) failed to implement a system of internal controls to protect customers' personal and financial information; (ii) failed to oversee and monitor the Company's internal controls system, resulting in inadequate internal controls that failed to protect customers' personal and financial information; and (iii) caused and/or consciously permitted the Company to conceal the full scope of the data breach and to provide inaccurate, untimely information about it. Defendant De Castro is a citizen of California.

27. Defendant Kenneth L. Salazar ("Salazar") is a Target director and has been since July 2013. Defendant Salazar is also Chairman of Target's Corporate Responsibility Committee and has been since at least May 2014 and a member of that committee since November 2013. Defendant Salazar knowingly and/or in conscious

disregard of his duties: (i) failed to implement a system of internal controls to protect customers' personal and financial information; (ii) failed to oversee and monitor the Company's internal controls system, resulting in inadequate internal controls that failed to protect customers' personal and financial information; and (iii) caused and/or consciously permitted the Company to conceal the full scope of the data breach and to provide inaccurate, untimely information about it. Defendant Salazar is a citizen of Colorado.

28. Defendant Solomon D. Trujillo ("Trujillo") was a Target director from 1994 to March 2014, when he left in the wake of one of the largest data breaches in history. Defendant Trujillo was also Chairman of Target's Corporate Responsibility Committee from at least April 2012 to at least January 2014. Defendant Trujillo and/or in conscious disregard of his duties: (i) failed to implement a system of internal controls to protect customers' personal and financial information; (ii) failed to oversee and monitor the Company's internal controls system, resulting in inadequate internal controls that failed to protect customers' personal and financial information; and (iii) caused and/or consciously permitted the Company to conceal the full scope of the data breach and to provide inaccurate, untimely information about it. Target paid defendant Trujillo the following compensation:

Fiscal Year	Fees Paid in Cash	Stock Awards	Option Awards	Change in Pension Value and Nonqualified Deferred Compensation	Total
2013	\$105,000	\$170,013	-	\$41,597	\$316,610
2012	\$105,000	\$90,055	\$71,477	\$32,165	\$298,697

Defendant Trujillo is a citizen of California.

29. The defendants identified in ¶¶15-17 are referred to herein as the "Officer Defendants." The defendants identified in ¶¶15, 18-28 are referred to herein as the "Director Defendants." Collectively, the defendants identified in ¶¶15-28 are referred to herein as the "Individual Defendants."

## **DUTIES OF THE INDIVIDUAL DEFENDANTS**

### **Fiduciary Duties**

30. By reason of their positions as officers and directors of the Company, each of the Individual Defendants owed and owe Target and its shareholders fiduciary obligations of trust, loyalty, good faith, and due care, and were and are required to use their utmost ability to control and manage Target in a fair, just, honest, and equitable manner. The Individual Defendants were and are required to act in furtherance of the best interests of Target and not in furtherance of their personal interest or benefit.

31. To discharge their duties, the officers and directors of Target were required to exercise reasonable and prudent supervision over the management, policies, practices, and controls of the financial affairs of the Company. By virtue of such duties, the officers and directors of Target were (and are) required to, among other things:

- (a) devise and implement a system of internal controls sufficient to ensure that the Company's customers' personal and financial information is protected;
- (b) monitor and oversee a system of internal controls sufficient to ensure that the Company's customers' personal and financial information is protected;
- (c) ensure that the Company timely and accurately informed customers regarding any breach of their personal and financial information;



(d) establish corporate governance and reporting structures effective to inform themselves about data security risks and enable them to oversee data security risk management;

(e) conduct the affairs of the Company in an efficient, business-like manner in compliance with all applicable laws, rules, and regulations so as to make it possible to provide the highest quality performance of its business, to avoid wasting the Company's assets, and to maximize the value of the Company's stock; and

(f) remain informed as to how Target conducted its operations, and, upon receipt of notice or information of imprudent or unsound conditions or practices, make reasonable inquiry in connection therewith, and take steps to correct such conditions or practices.

### **BREACHES OF DUTIES**

32. The conduct of the Individual Defendants complained of herein involves a knowing and culpable violation of their obligations as officers and directors of Target, the absence of good faith on their part, and a conscious or reckless disregard for their duties to the Company, which the Individual Defendants were aware or reckless in not being aware posed a risk of serious injury to the Company.

33. The Individual Defendants, because of their positions of control and authority as officers and/or directors of Target, were able to and did, directly or indirectly, exercise control over the wrongful acts complained of herein. The Individual Defendants also failed to prevent the other Individual Defendants from taking such illegal

actions. As a result, and in addition to the damage the Company has already incurred, Target has expended, and will continue to expend, significant sums of money.

**CONSPIRACY, AIDING AND ABETTING, AND CONCERTED ACTION**

34. In committing the wrongful acts alleged herein, the Individual Defendants have pursued, or joined in the pursuit of, a common course of conduct, and have acted in concert with and conspired with one another in furtherance of their common plan or design. In addition to the wrongful conduct herein alleged as giving rise to primary liability, the Individual Defendants further aided and abetted and/or assisted each other in breaching their respective duties.

35. The Individual Defendants engaged in a conspiracy, common enterprise, and/or common course of conduct. During this time, the Individual Defendants failed to timely and accurately inform customers regarding the full scope of the breach of their personal and financial information.

36. The purpose and effect of the Individual Defendants' conspiracy, common enterprise, and/or common course of conduct was, among other things, to disguise the Individual Defendants' violations of law, breaches of fiduciary duty, and waste of corporate assets, and to conceal adverse information concerning the Company's operations.

37. The Individual Defendants accomplished their conspiracy, common enterprise, and/or common course of conduct by allowing the Company to purposefully or recklessly conceal the scope of the data breach affecting at least seventy million customers. Because the actions described herein occurred under the authority of the

Board, each of the Individual Defendants was a direct, necessary, and substantial participant in the conspiracy, common enterprise, and/or common course of conduct complained of herein.

38. Each of the Individual Defendants aided and abetted and rendered substantial assistance in the wrongs complained of herein. In taking such actions to substantially assist the commission of the wrongdoing complained of herein, each Individual Defendant acted with knowledge of the primary wrongdoing, substantially assisted in the accomplishment of that wrongdoing, or is presumed to have acquiesced to the wrongdoing and was aware of his or her overall contribution to and furtherance of the wrongdoing.

#### **BACKGROUND**

39. Target is the second largest general merchandise retailer in the United States. The Company operates 1,797 stores in the United States and 124 stores in Canada.

40. Target's "Privacy Policy" acknowledges that the Company routinely collects personal information from its customers, including the customer's name, mailing address, e-mail address, phone number, driver's license number, and credit/debit card number. When customers use their debit cards to make a purchase at Target retail stores, they are required to enter the PIN associated with their bank account. Target promises its customers that it will, among other things, "*maintain administrative, technical and physical safeguards to protect your personal information*." When we collect or transmit

sensitive information such as a credit or debit card number, *we use industry standard methods to protect that information.*"

41. As discussed in detail below, notwithstanding Target's affirmative promise (and, thus, admitted duty) to protect its customers' personal and financial information, the Individual Defendants failed to ensure that Target (*would be able to*) protect this information for tens of millions of the Company's customers, exposing them to identity theft and other significant financial losses.

42. Identity theft occurs when one's personal information is wrongfully obtained without his or her knowledge. Armed with a one's personal or financial information, identity thieves can encode the victim's account information onto a different card with a magnetic strip, creating a counterfeit card that can be used to make fraudulent purchases. With the addition of a victim's PIN, a thief can use the counterfeit card to withdraw money from the victim's bank account.

43. Identity thieves can further harm their victims by using personal information to open new credit and utility accounts, receive medical treatment on their health insurance, or even obtain a driver's license. Once a person's identity has been stolen, reporting, identifying, monitoring, and repairing the victim's credit is a cumbersome, expensive, and time-consuming process. In addition to the frustration of having to identify and close affected accounts and correct information in personal credit reports, victims of identity theft often incur costs associated with defending themselves against civil litigation brought by creditors. Victims also suffer the burden of having difficulty obtaining new credit and must monitor their credit reports for future

inaccuracies, since fraudulent use of stolen personal information may persist for several years.

44. Annual monetary losses from identity theft are in the billions of dollars.

According to the President's Identity Theft Task Force Report dated October 21, 2008:

In addition to the losses that result when identity thieves fraudulently open accounts or misuse existing accounts, ... individual victims often suffer indirect financial costs, including the costs incurred in both civil litigation initiated by creditors and in overcoming the many obstacles they face in obtaining or retaining credit. Victims of non-financial identity theft, for example, health-related or criminal record fraud, face other types of harm and frustration.

In addition to out-of-pocket expenses that can reach thousands of dollars for the victims of new account identity theft, and the emotional toll identity theft can take, some victims have to spend what can be a considerable amount of time to repair the damage caused by the identity thieves. Victims of new account identity theft, for example, must correct fraudulent information in their credit reports and monitor their reports for future inaccuracies, close existing bank accounts and open new ones, and dispute charges with individual creditors.

45. The significant impact of identity theft on consumers' personal well-being, and the extreme financial ramifications that can result from the failure to secure one's personal information, has led to the enactment of numerous privacy-related laws designed to protect consumer information and disclosure requirements, including: (i) the Gramm-Leach-Bliley Act; (ii) the Fair Credit Reporting Act; (iii) the Fair and Accurate Credit Transactions Act; (iv) the Federal Trade Commission Act, 15 U.S.C. §§41-58; (v) the Driver's Privacy Protection Act; (vi) the Health Insurance Portability and Accountability Act; (vii) the Privacy Act of 1974; (viii) the Social Security Act Amendments of 1990;

(ix) the E-Government Act of 2002; and (x) the Federal Information Security Management Act of 2002.

**THE INDIVIDUAL DEFENDANTS WERE WELL AWARE OF THE  
CATASTROPHIC DANGERS INHERENT IN DATA BREACHES**

**Target Had Considered, but Abandoned, a Safer Payment Card System More than  
a Decade Ago**

46. As early as 2001, Target officials knew that the Company's customers' credit and debit card information was vulnerable to misappropriation. Target, like virtually all U.S. retailers, uses a POS system based on magnetic stripes on credit cards.<sup>2</sup> The magnetic strip is read by the card reader, which sends data to a server that confirms that the card has sufficient funds available for the payment and informs the customer's bank of the amount charged on the card. The data on the magnetic strip never changes. This opens up vulnerabilities because once the card data is improperly obtained, the criminals can quickly and easily produce fraudulent cards.

47. U.S. retailers are outliers. Companies in Europe and Canada commonly use chip-based credit cards, which encrypt the credit card data before sending it to the server, and create unique codes for each transaction. This better safeguards stolen data by making it far more difficult to counterfeit a card and make fraudulent purchases.

48. Beginning in 2001, Target attempted to convert its stores to chip-based card POS readers and transition Company-issued credit cards to a chip-based format. Former

---

<sup>2</sup> In the interest of brevity, "credit card" as used in the Complaint refers to credit cards, debit cards, Target proprietary payment cards, and all other swipeable plastic payments cards.

CFO defendant Mulligan acknowledged that there were "operational, financial and marketing benefits" to this program.<sup>3</sup> Chip-based cards require different POS card readers that operate a few seconds slower than magnetic strip cards. Target installed 37,000 of these POS terminals. However, despite this investment and the known vulnerabilities of magnetic swipe POS, Target discontinued the chip-based card readers in 2004. A group within Target led by then-CEO defendant Steinhafel were concerned that the few seconds of extra delay was not worth the added security. Thus, Target reverted to the extremely vulnerable magnetic strip cards.

49. Since that time, "[a] lot of the fraud has migrated from international markets to the U.S. because the U.S. is the weakest link," said Rick Oglesby, an Aite Group LLC payment industry analyst. One and a half billion smart cards are estimated to be in circulation, in use in eighty countries other than the U.S. Target's Canada stores use smart-card technology, and they have not suffered data breaches like Target's U.S. stores, as explained further *infra* at ¶¶73-74.

#### **Target Suffered a Massive Data Security Hack in 2009**

50. In the early 2000s, a group of criminals led by Alberto Gonzalez ("Gonzalez") exploited vulnerabilities in the IT security of many retailers. The hackers used virtually the same techniques as those at issue here to obtain data from more than 170 million cards. Gonzalez and his associates hacked into companies' POS terminals,

---

<sup>3</sup> Paul Ziobro and Robin Sidel, *Target Tried Antitheft Card*, The Wall Street Journal, Jan. 20, 2014, <online.wsj.com/news/articles/SB10001424052702304027204579332990728181278>.

migrated within their servers to locate customers' personal financial information, exfiltrated the information, and then sold it to illegal operations in Eastern Europe.

51. Gonzalez hacked Target between 2005 and 2007. After Gonzalez pled guilty in 2009, a Target spokeswoman admitted that various payment card numbers had been stolen from Target by Gonzalez in or around 2007. In 2009, *two years after that attack*, Target officials were *still* unsure how many customers' credit cards had been affected and remained unable to even understand how it had happened in the first place. Gonzalez was sentenced to up to twenty-five years in prison, but the vulnerabilities which enabled his hacking techniques have lived on at Target because of the Individual Defendants' blasé approach to dealing with the ever-expanding threat of cyber attacks. Former CEO defendant Steinhafel admitted that he knew about the ramifications of liability from cyber attacks due to previous breaches like the Gonzalez attack, as discussed *infra* at ¶120.

#### **The Individual Defendants Were Repeatedly Warned of the Risks of Cyber Attacks**

52. In addition to the internal red flags indicating that Target's information security systems and controls were woefully inadequate, the Individual Defendants received repeated warnings from U.S. government agencies and other reputable sources regarding the damages a successful data breach could wreak upon the Company. The recent wave of cyber attacks on American corporations prompted warnings from every direction. And as Internet businesses continued expanding in the 2000s, many prominent researchers acknowledged huge vulnerabilities in many corporate networks, including Target's.



53. On August 27, 2007, Dr. Neal Krawetz, a data security expert working for Hacker Factor Solutions, publicly disclosed a White Paper titled "Point-of-Sale Vulnerabilities," which warned of the reality that a POS data breach at Target would result in substantial damages to the Company. The White Paper identified Target as an example of the potential ramifications a POS data breach could have at a major retailer, estimating that as many as *fifty-eight million card accounts* could be compromised if Target's POS system was breached.

54. In 2008, the Verizon Business RISK Team published the first of its annual Data Breach Investigations Reports. The 2008 report reviewed the results of forensic investigations of tens of thousands attempted data breaches from 2004 to 2007. The 2008 report reached numerous important conclusions about data security and brought attention to Target's vulnerability to a massive data breach, explaining the affirmative action that was necessary to protect Company customers' data, including the following:

- 35% of the data breaches investigated occurred in retail businesses, often the path of least resistance for cyber criminals;
- External sources accounted for more than 73% of the confirmed data breaches, and the external actors often gained access via a remote vendor's credentials first, and then entered the victim's high-value servers.
- IP addresses from Eastern Europe and Russia are commonly associated with the compromise of POS systems.

- The majority of data breaches occurred because a malicious code was remotely planted by a hacker and resulted in a compromised system security.
- Hackers often used targeted attacks against certain retail and food and beverage companies upon learning that those companies run certain vulnerable software.
- Hackers successfully compromised payment card data in 84% of all reported data breaches.
- "The fact of that matter is that though most organizations have the technologies, people and know-how required to detect and respond to data compromise events, they seldom do so. In 82 percent of cases, our investigators noted that the victim possessed the ability to discover the breach had they been more diligent in monitoring and analyzing event-related information available to them at the time of the incident. The breakdown is in the process. What these organizations seem to lack is a fully proceduralized regimen for collecting, analyzing, and reporting on anomalous log activity."
- 87% of the data breaches could have been avoided if reasonable security controls had been in place at the time of the incident.

- In 59% of the data breaches, the organization had security policies and procedures established to secure their systems, but these plans were not implemented via actual procedures.

55. Verizon has dutifully published a data breach investigations report every year since 2008, and each year the report has repeated similar warnings about attacks similar to the one perpetrated against Target. In the 2013 report, the last report to go to print before the Target data breach, the authors concluded that the most common form of data breach resulted from opportunistic, external hackers exploiting weak or stolen credentials for a financial motive on retail targets. The author exhorted companies to "focus on better and faster detection through a blend of people, processes and technology" in light of the increase in the average length of time that a breach went undetected.

56. In 2013, Verizon also published a special report of the data breach investigations that occurred in the retail sector. The report warned that retail attacks were eminently predictable: 97% involved payment systems, and a majority involved POS servers. Again the report warned retailers to change the default passwords built into new hardware and reiterated that most attacks used malware on a target POS machine after gaining access through other means. Retailers were also instructed to use strong authentication on all POS systems because "easily guessable passwords make the hacker's job much easier."

57. In May 2013, the Department of Homeland Security issued a warning that it was "highly concerned about hostility against critical infrastructure organizations."

The warning was issued by an agency called ICS-Cert, which monitors attacks on computer systems that run industrial processes.

58. The Individual Defendants were further put on notice of data security risks as a result of their own experiences in separate businesses that had experienced data breaches. As demonstrated *infra* at ¶¶140, defendants Steinhafel, Johnson, Trujillo, Mulcahy, Austin, Darden, Rice, Stumpf, Baker, and De Castro each signed documents and/or otherwise encountered and understood the importance of data security issues as a result of their service on boards of other companies. By signing U.S. Securities and Exchange Commission ("SEC") documents attesting to the risks inherent in data breaches, the Individual Defendants recognized and understood the need for strong data security risk governance and controls, yet (as discussed below) failed to act to prevent the massive data breach that struck Target.

59. Industry analysts have called attention to the failures of boards of directors to take appropriate action to prevent or mitigate data breaches. For instance, on May 12, 2012, Global Cyber Risk LLC published its third survey of governance relating to enterprise security. It concluded, for the third time, that "boards are not actively addressing cyber risk management.... Boards still are not undertaking key oversight activities related to cyber risk, such as reviewing budgets, security program assessments, and top-level policies; assigning roles and responsibilities for privacy and security; and receiving regular reports on breaches and IT risks." The report noted the failure of boards to ensure that their companies have full-time personnel in CISO/Chief Security Officer ("CSO"), Chief Privacy Officer, or Chief Risk Officer ("CRO") roles, and failure

to eliminate the segregation of duties problems that often occur when CISOs have responsibility for both privacy and security but report to the CIO. The report recommended twelve major actions that boards should take to improve enterprise security, the first of which is to establish a Risk Committee separate from the Audit Committee with responsibility for enterprise risks and comprised which is of directors with security and IT governance and cyber risk expertise. The report quotes the *Independent Director*, which concluded that management of information risk is central to the success of any organization operating today. For directors, this means the boards performance is increasingly being judged by how well the company measures up to internationally accepted codes and guidelines on preferred information assurance practice.

**THE INDIVIDUAL DEFENDANTS FAILED TO IMPLEMENT AND OVERSEE  
A SUFFICIENT SYSTEM OF INTENRAL CONTROLS**

60. Despite all of the red flags and warnings that were obvious to the Individual Defendants leading up to the data breach at Target, the Company remained utterly vulnerable to a data breach because of Board-level failures to institute reporting and control systems and/or to monitor the deficient systems and procedures that were in place.

**Target's Corporate Governance Was Woefully Inadequate to Prevent or Mitigate  
Data Breaches**

61. The first and most obvious deficiency was the Board's failure to find and staff directors who were capable of understanding and addressing data security problems and risks. In response to the data breach, the Board acknowledged that it is the

responsibility of the entire Board to oversee risk. Yet, the Target Board has no written, specific governance, procedures, or division of responsibilities for overseeing risk of any kind, particularly data security risks—indeed, the word "risk" does not even appear in the Board Governance Guidelines.<sup>4</sup> While the Guidelines require the Board to have broad perspective, experience, and knowledge, not one member of Target's Board had specific expertise in or knowledge of data security issues.<sup>5</sup> The Board as a whole failed to institute corporate governance to oversee data security risk and/or to monitor the unwritten procedures it purportedly follows with regard to data security risks.

62. The Board has five committees: Audit, Compensation, Nominating and Governance, Corporate Responsibility, and Finance. The descriptions for membership on each committee outline the responsibilities of the committee. None of the committees explicitly assume responsibility for data security risk management. Ostensibly, the Audit Committee is charged with oversight of information security. A review of the Audit Committee responsibilities and its members, however, makes clear that the Audit Committee was mainly concerned with financial audits, while its risk management

---

<sup>4</sup> See, e.g., Target's Proxy Statement on Form DEF 14A filed with the SEC on April 29, 2013 ("2013 Proxy") ("The primary responsibility for the identification, assessment, and management of the various risks that we face belongs with management. The Board's oversight of these risks occurs as an integral and continuous part of the Board's oversight of our businesses.").

<sup>5</sup> The Company's 2013 Proxy does not discuss the knowledge or expertise of the Board with regard to data security or cyber risks. Only after the data breach, in Target's Proxy Statement on Form DEF14A filed with the SEC on May 19, 2014, did the Board begin to discuss data security issues.

responsibilities were (at best) secondary. "Risk Assessment" is mentioned in one paragraph in the Audit Committee Charter:

**"C. Risk Management; Oversight of Internal Audit**

1. **Risk Assessment.** Review and discuss with management its approach to risk assessment and risk management, including the risk of fraud, and the commitment of internal audit resources to audit the Corporation's guidelines, policies and procedures to mitigate identified risks."

The remainder of the risk management duties involve audits. The words "data security" or "information security" (or anything close) do not appear in the Audit Committee Charter. The Audit Committee members did not have and did not exercise adequate oversight over data security risks. As discussed *infra* at ¶125, Institutional Shareholder Services ("ISS") urged the ouster of the members of Target's Audit and Corporate Responsibility Committees because of their utter failure to ensure appropriate management of the data security risks that damaged the Company.

63. The background and (lack of) experience of the members of the Audit Committee further call into doubt the ability of the Individual Defendants to effectively oversee Target's information security procedures and personnel. None of the members of the Audit Committee have any expertise or specialized knowledge in data security. Chairman defendant Austin has a background in accounting; defendant Baker has a background in marketing, sales, and management; defendant Minnick has an MBA and a marketing and sales background; and defendant Rice has a background in finance.<sup>6</sup> The

---

<sup>6</sup> See 2013 Proxy.

Audit Committee was built for audit and financial oversight, but it was woefully unqualified and unprepared for, and unaccountable to, the Company with respect to its responsibility to oversee data security risks.

64. No other committee or committee members were any better-suited to monitor, oversee, and protect against data security risks at Target. The Nominating and Corporate Governance Committee ("Corporate Governance Committee") was charged with "[r]eview[ing] and assess[ing] as necessary the adequacy of the Corporation's Corporate Governance Guidelines and any similar policies and recommend[ing] any proposed changes to the Board for approval." But no specific corporate governance guidelines for data security existed. In addition, as discussed above, the Corporate Governance Committee failed to nominate Board members with backgrounds in data and IT security, further weakening the ability of the Board to craft appropriate corporate governance and oversee data security risks.

65. The members of the Corporate Responsibility Committee were also unprepared to oversee data security risks themselves. The Corporate Responsibility Committee was charged with "[a]ssist[ing] management in identifying and determining an appropriate response to emerging public issues critical to achievement of the Corporation's strategic objectives related to its constituencies, including its customers, team members, shareholders and communities." Yet the clearly identified public issue of data security, which had resulted in the breach of credit card information of Target's customers only a few years earlier, remained an unresolved risk to Target and its customers.



66. Similarly, the members of the Finance Committee and Compensation Committee were also unprepared and unable to equip Target with the ability to prevent or mitigate a data security breach.

67. The Individual Defendants were fully aware of the ramifications of these failures to keep customers' data secure and knew that the Company would be subject to costly government enforcement actions and private litigation in the event of a data breach. Indeed, they acknowledged (or at least gave lip service to) these risks in the risk disclosures statements in the Company's Annual Report on Form 10-K filed with the SEC on March 20, 2013:

*If we experience a significant data security breach or fail to detect and appropriately respond to a significant data security breach, we could be exposed to government enforcement actions and private litigation. In addition, our guests could lose confidence in our ability to protect their personal information,* which could cause them to discontinue usage of REDcards, decline to use our pharmacy services, or stop shopping with us altogether. *The loss of confidence from a significant data security breach involving team members could hurt our reputation,* cause team member recruiting and retention challenges, increase our labor costs and affect how we operate our business.

68. This attempt to mitigate securities fraud liability and appease the SEC was not, however, the product of a substantive recognition of data security risks. Target's reporting and internal controls systems in place before the data breach did little (if anything) to prevent the "significant" risk that data breaches presented for Target and its customers. Leading up to the breach, Target did not even have a CISO or a CSO, and the Company has only hired one such officer even now in this face of the breach. Target also did not and still does not have a CRO. Target's CIO, defendant Jacob, resigned

immediately after the breach. The manager of Target's security operations, Brian Bobo, left the Company in October 2013, leaving a crucial post vacant in the month before the breach. Target did not have appropriate personnel in key director and officer positions who could have prevented the data breach. The corporate governance in place left the castle unlocked with no one guarding the doors.

**Target's Data Security Practices Displayed Easily Exploitable Weaknesses to Hackers**

69. Target's data security procedures (or lack thereof) left the Company vulnerable to hacking attacks, and it came to be viewed as an easy target. As the Verizon 2013 Data Breach Investigations Report found, "some organizations will be a target *regardless* of what they do, but most become a target *because* of what they do." The Verizon report discussed so-called "[o]ppportunistic attacks," where "[t]he victim isn't specifically chosen as a target; they were identified and attacked because they exhibited a weakness the attacker knew how to exploit." Target left a number of clues to hackers about ways in which they could access the Company's customer cardholder information.

70. Target publicly displayed data from its vendors that contained metadata, exposing some of its vulnerabilities. As discussed below, the hackers did not break directly into Target's servers, but gained access via the servers of a Pennsylvania-based company Fazio Mechanical Services Inc. ("Fazio"), heating, ventilation and air-conditioning ("HVAC") vendor that operated Target's air-conditioning and heating. Target posted an excessive amount of information about its servers on its publicly accessible Facilities Management webpage. Data connected to servers on these pages

enabled any curious person with an Internet connection and some free software to find out that Target was still running Microsoft Office 2007 in June 2011, and that the domain on Target's servers where this was run was "\\TCMPSPRINT04P\." Indeed, some investigators have identified the name of a similar server from which the hackers were able to exfiltrate the POS data. The hack occurred and succeeded because of the hackers' knowledge of Target servers, which they gleaned from information that Target left publicly available.

71. Target also failed to inquire about the IT security used by its vendors. As discussed below, Fazio admitted that it was "the victim of a sophisticated cyber attack operation," and that it should have been no surprise. Fazio's primary method of detecting malicious software on its internal system was the free version of Malwarebytes Anti-Malware. Not only does this product's licensing agreement prohibit corporate use, but the free version offers no real-time protection against threats. Effectively, the backdoor to Target's servers was guarded by a free piece of antivirus software barely sufficient to protect an individual's home computer. Yet, Target did not inquire about Fazio's security measures and took no steps to prevent breaches like this.

72. Finally, Target failed to eliminate default accounts on its system, effectively permitting hackers to move from room-to-room once they gained access inside. Default account names and passwords are commonly used by Windows software to complete routine tasks. But, as one industry expert asserts, the hackers leveraged a default account to order Target servers to move the pilfered data around the system until it could be safely exfiltrated.

### **Target's Expansion into Canada Illuminates Weaknesses in the Company's POS System**

73. Before the data breach, Target had recognized weaknesses in its POS. In January 2011, Target announced that it would open stores in Canada, expanding beyond the U.S. for the first time. The initial announcement predicted that around 200 stores would be opened in total, with 100-150 of them ready in 2013.

74. Target created a home-grown software information system for processing POS payments for its domestic stores. This system, called the "Domain Center of Excellence," was an imperfect one, a product of the haphazard and unpredictable growth that Target has experienced in the past fifty years.<sup>7</sup> This system is housed on Windows software, where many vulnerabilities have been found in recent years.<sup>8</sup> When Target expanded into Canada, it concluded that the home-grown system should not be used and purchased a new system called "Retailix" for its Canadian stores. Sources report that Target now plans to roll out the Retailix POS into U.S. stores at some point in the future.

75. In early 2013, the federal government and private research firms distributed memoranda regarding the emergence of new types of malicious computer code targeting payment terminals, according to a former employee who spoke with *The Wall Street*

---

<sup>7</sup> See *A First Look at the Target Intrusion, Malware*, Krebs on Security, Jan. 15, 2014.

<sup>8</sup> See, e.g., the seventy vulnerabilities listed by CVE Details available at [http://www.symantec.com/security\\_response/writeup.jsp?docid=2013-121909-3813-99&tabid=2](http://www.symantec.com/security_response/writeup.jsp?docid=2013-121909-3813-99&tabid=2).

*Journal*.<sup>9</sup> Target and other retailers saw a "significant uptick" in malware attempting to enter their systems in 2013. And at least two months before the attack, Target computer security staff raised concerns about vulnerabilities in the payment card system to their superiors. One Target analyst called for a more thorough security review of the payment system, but his request was brushed off by senior Target employees.

76. The suggested review also came as Target was updating its payment terminals, a process that often leaves security risks vulnerable because computer security experts have little time to plug the holes in the system. The request for the review came immediately before the important Black Friday weekend.

77. According to a reporter who wishes not to be named, at some point in 2013, Target considered updating its domestic POS systems. Target knew there was a vulnerability in the POS systems that permitted credit card data to travel between the POS device and the register before it was encrypted and sent off to the clearinghouse for approval. The Company's security team knew about this vulnerability and knew it that involved sensitive cardholder information.

78. Essentially, in the weeks before the data breach, Target's customers' information was held in an unlocked, unprotected castle with vulnerabilities on all sides. The Individual Defendants knew that Target had been previously hacked, it had received

---

<sup>9</sup> Danny Yadron, Paul Ziobro, and Devlin Barrett, *Target Warned of Vulnerabilities Before Data Breach*, Feb. 14, 2014, <[online.wsj.com/news/articles/SB10001424052702304703804579381520736715690](http://online.wsj.com/news/articles/SB10001424052702304703804579381520736715690)>.

warnings that hackers were interested in POS servers of retail companies, had serious vulnerabilities on its POS servers, and would suffer massive damages if and when a data breach were to occur. Yet, the Company, under the direction of the Individual Defendants, had insufficient corporate governance, unprepared personnel, and vulnerable procedures in place. Target was not unlucky—it was unprepared and unprotected.

**THE INDIVIDUAL DEFENDANTS' FAILURE TO PROTECT CUSTOMERS' PERSONAL INFORMATION LEADS TO RECORD-SETTING DATA BREACH**

79. Hackers conducted a four-part attack akin to breaking into a bank via the building next door. First, they gained access to Target's system through a third-party's servers. Second, they installed software that recorded the financial information of tens of millions of credit cards. Third, they moved the financial information to a place within Target's system where it could be exported. And fourth, they exfiltrated the data to a computer in eastern Europe where they could access it for illicit, personal gain.

80. The U.S. Senate reviewed the events of the Target attack using an intrusion "kill-chain" framework, an analytical tool commonly utilized in the information security world. A kill-chain analysis is premised on the fact that a hacker must succeed at every step of the chain, but if the target stymies the attack at any of the points along the way, the attack will not succeed. At each of these four stages, the Senate report identified a glaring mistake made by the Individual Defendants that could and would have prevented the attack. The failure to prevent the attack at any of these four stages demonstrates the Individual Defendants' failure to implement and monitor sufficient internal controls related to information security.

81. Target is a massive corporation with more than 1,700 stores in the U.S., more than 360,000 employees, and revenue of more than \$72 billion in 2013. Like every business in the digital age, Target's servers connect wide-ranging operations that coordinate everything from sales to lighting to employee payroll information. Target operates two massive data centers in Minnesota: the Target Technology Center ("TTC") in Brooklyn Park, Minnesota, and the Target Technology Center Elk River ("TTCE") in Elk River, Minnesota. Because servers are so important to large organizations, and so sensitive, many government agencies, major banks, and technology companies often build their own security operations centers ("SOCs").

82. Target built its own SOC and ran its domestic security operations out of the 6th floor of the City Center building in downtown Minneapolis. The Company also contracted with a security team in Bangalore, India. Both teams used a recently purchased, \$1.6 million malware detection tool from FireEye Inc. ("FireEye"), which that monitored security threats to Target's servers and network. The procedure for security alerts was that Bangalore would monitor alerts around the clock. When important alerts arose, Bangalore would notify Minneapolis, and Minneapolis analysts would act on the alerts. As discussed below, however, this process and the relevant individuals failed to protect Target.

#### **Target Failed to Limit Access to Its Servers**

83. The hackers first gained access to Target's servers using a connection from Fazio, a HVAC company based in Pennsylvania. In order to coordinate its massive operations, Target provides connections to its servers to many third-party contractors.

Fazio had a data connection to Target services for "electronic billing, contract submission and project management." It is common for HVAC companies to monitor energy consumption and heating for stores remotely. Such vendors often need remote access to do maintenance and troubleshoot glitches or connectivity issues. The problem is not that Fazio had remote access, it is that the remote access was not well-guarded.

84. The hackers began their attack on Target in late 2013 by attacking Fazio. Although details have not been publicly confirmed, Fazio has admitted it was the "victim of a sophisticated cyber attack" that purportedly stole its log-in credentials. One industry expert cited two confidential sources who stated that the hackers used password-stealing malware in an e-mail attack.

85. Regardless of the precise tool used, the hackers were likely to be successful because Fazio's credentials were not well protected. Fazio's primary method of detecting malicious malware was the free version of Malwarebytes Anti-Malware. Although this program may be useful in some contexts it was utterly inadequate here for two reasons. First, the product is not intended for corporate use, and its licensing agreement prohibits corporate use. Second, the free version does not offer real-time protection against threats. Like a scanner on a personal computer, the free version will only search for malware if someone runs the program. Otherwise, no alerts or protection are activated when hackers attack. No one at Fazio realized an attack had occurred until Fazio was visited by the U.S. Secret Service.

86. The successful attack against Fazio became a problem for Target only because Target enabled a back-door entry into its servers. Target leaves massive amounts



of internal documentation about its vendors on public websites. There are at least three sites that connect Fazio and Target. First, nearly all Target contractors have access to its external billing system, Ariba. Second, most contractors have access to Target's project management and contract submissions portal, Partners Online. Third, Fazio had access to Target's Property Development Zone portal.

87. While certain facts are still being revealed about exactly how the hackers navigated from Fazio's connection to Target into more sensitive areas within Target's network, one former Target network expert has theorized:

I know that the Ariba system has a back end that Target administrators use to maintain the system and provide vendors with login credentials, [and] I would have to speculate that once a vendor logs into the portal they have active access to the server that runs the application. Most, if not almost all, internal applications at Target used Active Director ("AD") credentials and I'm sure the Ariba systems was no exception. I wouldn't say the vendor had AD credentials but that the internal administrators would use their AD login to access the system from the inside. This would mean the sever [sic] had access to the rest of the corporate network in some form or another.

88. In other words, once the hackers obtained Fazio's login credentials, they had access to a connection to all of Target's data, which was protected only by a username and password. The existence of this back-end entry was not publicly known, but it was likely routinely accessed by Target network administrators.

89. Hackers, by nature, are adept at gaining access to information and servers that otherwise should be protected, but Target enabled such access by two fatal mistakes: (i) failing to require two-factor identification; and (ii) publicly posting information about the architecture of its servers. The U.S. Senate report makes clear that both of these failures represented missed opportunities to thwart the hackers in the kill chain.

90. First, Target failed to require two-factor identification. Security industry expert Brian Krebs ("Krebs"), who first broke the Target data breach report, spoke with a source who managed Target vendors for a number of years. This source stated that only "in rare cases" would Target have required a vendor to use two-factor authentication, or a one-time token (a similar method). "Only the vendors in the highest security group—those required to directly access confidential information—would be given a token, and instructions on how to access that portion of the network," the source stated, speaking on the condition of anonymity. "Target would have paid very little attention to vendors like Fazio, and I would be surprised if there was ever even a basic security assessment done of those types of vendors by Target."

91. A username and password is a form of single-factor identification. Requiring a PIN, and a one-time code (token) e-mailed from Target's administrators, are examples of two-factor authentication. Because Target used single-factor authentication for its vendors, the hackers were able to gain access to Target's servers with only the pilfered username and password.

92. Two-factor authentication is widely recognized as an essential tool and a best practice for network protection. The Payment Card Industry ("PCI") Security Standards Council ("SSC"), an industry group that regulates security among companies that accept and store credit card information, publishes a list of Data Security Standards (DSS). The PCI DSS are an objective framework to assess network security. They also impose requirements that, if not met, can result in massive liability for violators. PCI DSS requirement 8.3 requires two-factor authentication for all parties with remote access

to a network that holds PCI information. Although Target was certified as PCI-compliant in September 2013, many commentators have concluded that Target likely will be found retroactively non-compliant, and in any event, that PCI compliance alone is not enough. A PCI report regarding the Target breach is expected to be forthcoming.

93. **Second**, Target published massive amount of information about its network and its vendors online. Security industry expert Krebs noted that simple searches on Google turned up pages with a wealth of information about the identity of Target suppliers and how they submit payment and work orders. By scanning some of these publicly available files, Krebs was able to determine that a Target employee with the Windows username "Daleso.Yadetta" was running Microsoft Office 2007 in June 2011 in the Windows domain of "\\TCMPSPRINT04P\." A search on LinkedIn demonstrates that Daleso Yadetta is a reporting analyst at Target based in Minneapolis.

94. As the U.S. Senate report found: "[H]owever the attackers actually leveraged their access to this vendor's system to enter Target's network, less security at the perimeter of Target's network may have contributed to the attackers' success in breaching the most sensitive area of Target's network containing cardholder data." With the benefit of information publicly provided by Target, and single-factor identification, only a password stood between hackers and the financial information of tens of millions of Americans.

### **Target Failed to Prevent or Detect the Installation of Malware**

95. According to sources who spoke to Krebs, the hackers installed Malware on Target servers at some point prior to November 27, 2013.<sup>10</sup> These sources state that "ttcpscli3acs" is the name of the Windows computer name/domain used by the malware planted at the Target stores, "Best1\_user" was the username, and "BackupU\$r" was the password. Krebs uploaded the results of a search for this malware run on "ThreatExpert.com," a malware scanning service. Krebs' source also stated that this malware is the same as a malware strain known as "Reedum."<sup>11</sup> Krebs and others believe that the malware is nearly identical to a piece of malware sold on cybercrime forums called "BlackPOS." BlackPOS is designed to be installed on POS devices and record data from cards swiped on them—not appreciably different than the attack breach Target suffered years ago at the hands of Gonzalez. BlackPOS can be purchased online from cybercrime forums for around \$2,000. In effect, a \$2,000 piece of software and a bit of technical know-how was all that was needed to open the vault to Target's consumers' card information.

96. The hackers had good reason to choose "Best1\_user" as the username to install the malware—it is the same username that is automatically installed with an IT management software suite called "Performance Assurance for Microsoft Servers." As

---

<sup>10</sup> See Krebs First look. Note the report on "Reedum" also identifies the same windows service name: POSWDS. See Symantec report available at [http://www.symantec.com/security\\_response/writeup.jsp?docid=2013-121909-3813-99&tabid=2](http://www.symantec.com/security_response/writeup.jsp?docid=2013-121909-3813-99&tabid=2).

<sup>11</sup> *Id.*

discussed above, Target ran its U.S. servers on vulnerable Windows programs, unlike the more recently built Canadian ones. Target executives and directors approved the use of Windows-based servers even though they knew they were risky. According to a reporter who wishes not to be named, Target employees explained this risk, and high-level employees labeled it "risk accept."

97. The Performance Assurance software is made by a company called BMC Software ("BMC"). BMC explains that the "Best1\_user" account is used to run routine maintenance of the software. However, BMC warns against adding the Best1\_user account to groups or otherwise failing to limit its permissions. Various IT security experts believe that this account was used by attackers to gain access to Target's customer data.

98. Within days of the installation of the malware, the hackers deployed their custom-made code. According to a source who spoke with *Bloomberg Businessweek*, on November 30, 2013, Target's FireEye security system spotted the malware and triggered its first alert: "malware.binary."<sup>12</sup> Target had spent \$1.6 million on the FireEye malware detection tool, and it alerted Target's security team in Bangalore, India, that malicious malware was being uploaded onto the Company's system. The Bangalore team dutifully

---

<sup>12</sup> Michael Riley, Ben Elgin, Dune Lawrence, and Carol Matlack, *Missed Alarms and 40 Million Stolen Credit Card Numbers: How Target Blew It*, Bloomberg Business Week, Mar. 13, 2014, <http://www.businessweek.com/articles/2014-03-13/target-missed-alarms-in-epic-hack-of-credit-card-data>.

elevated the issue, alerting Target's higher level security team in Minneapolis. And then Target, under the direction of the Individual Defendants, did nothing.

99. More than ten former Target employees and eight people with specific knowledge of the attack told *Bloomberg* that, despite the alarms, Target did not respond. The alerts were "the most urgent on FireEye's graded scale."<sup>13</sup> Yet, Target stood by and did nothing.

100. The alerts continued. The hackers inserted more versions of the same malware. Some security researchers believe the hackers used as many as five versions of malware. Each time, FireEye again sent out its most urgent alert. Target's system also recognized the addresses for servers where the hackers wanted to send information, but no action was taken by any Target representative.

101. Worse, Target employees disabled the automatic response that was programmed into FireEye. FireEye had an option to automatically delete malware as it is detected. But according to two individuals who audited FireEye's performance after the breach and spoke with *Bloomberg*, Target's security team turned off the automatic response function. These were warnings and protection systems that functioned properly, but because of the failed internal procedures and ineffective controls, Target missed the chance to stop the breach while it was in its infancy.

---

<sup>13</sup> *Id.*

102. Not only did FireEye reveal the malicious files, Target's antivirus system, Symantec Endpoint Protection, also identified suspicious behavior during the same period. The Symantec Endpoint Protection alerts pointed to the same server identified by the FireEye alerts. Any properly-functioning data security team would have understood that Target was under attack.

103. But Target's data security was not normally-functioning. Target security employees responsible for running FireEye viewed it with skepticism and did not give it adequate attention. Further, SOC manager Brian Bobo left the Company in October 2013, leaving a crucial post vacant. And, as detailed above, Target lacked a CISO, a C-level risk officer, and effective governance, procedures, and compliance controls to ensure that the data alerts were given due attention and appropriately addressed.

104. Because no one attended to the alerts, the malware began copying the credit card data of Target customers. On December 2, 2013, the malware began transmitting payloads of stolen data to a file transfer protocol server. This, too, set off alerts in Target's security system that went unnoticed or were not acted upon.<sup>14</sup> For two weeks, the malware sent data to three different U.S. staging points. The malware only transmitted data during U.S. working hours in order to obscure the data in regular working-hour traffic.

---

<sup>14</sup> *Id.*

105. From those staging points, the data was sent to a virtual private server in Russia, where the hackers could access the data. The hackers were first able to remove the data on December 2, 2013. For two weeks, hackers continued pilfering credit card numbers. In total, they took eleven gigabytes of information, amounting to 110 million records of Target customers' personal and financial information.

106. Had Target's security team followed up on the FireEye alerts, even within a few days or weeks of the attacks, they may have had a chance to catch the cyber criminals. The uploaded malware included the user names and passwords for the thieves' staging servers embedded in the code. Target could have signed into its own servers, located in the U.S., and seen the stolen data sitting there waiting for the hackers' daily transmission. But even weeks after the attack began, Target still had not realized it was being hacked.

107. Target also failed to review activity on its own servers, which appears to violate industry security standards. The PCI DSS require vendors to monitor the integrity of critical system files.<sup>15</sup> One common procedure for doing this is called "white listing," whereby only approved processes are allowed to run on a machine. A white listing of Target's servers during the breach would have produced another alert that suspicious

---

<sup>15</sup> See PCI Data Security Standard Version 3.0, Requirement and Security Assessment Procedures, at 96 (Nov. 2013), [www.pcisecuritystandards.org/documents/PCI\\_DSS\\_v3.pdf](http://www.pcisecuritystandards.org/documents/PCI_DSS_v3.pdf). The PCI council often retroactively revokes certifications; a post-breach review of Target's PCI compliance has not yet issued. See, generally Verizon Data Breach Investigations Report 2012 at 57 (2012).



processes were running. But the Individual Defendants did not ensure that there were people, policies, or procedures in place that required white listing or any of the other common procedures that could have prevented the data breach.

108. Not only did Target fail to follow up on the alerts in a timely manner, no Target representative ever looked at the alerts. Without outside intervention, Target would have never known that its customers' credit card data had been stolen right from under its nose. Target had no idea it was attacked until the U.S. Secret Service informed the Company about it on December 12, 2013.<sup>16</sup> Without external notification and assistance, the Target breach would have continued for months.

#### **THE PUBLIC LEARNS OF THE BREACH BEFORE COMPANY OFFICIALS DISCLOSE IT**

109. Some Target customers noticed fraudulent transactions on their cards in early December 2013, more than a week before Target publicly acknowledged any issue. One customer in Minneapolis saw an unusual charge, a \$1,290 plane ticket from Lagos, Nigeria, to Johannesburg, South Africa, and contacted her card company regarding the fraudulent charge.<sup>17</sup> But it would be another week until Target admitted any issue concerning the compromised personal and financial information of its customers.

---

<sup>16</sup> The earliest known recognition of the attack comes in the form of an upload of the malware used in the attack, bearing the name of the perpetrator, to a data security website on December 11, 2013. See, Brian Krebs, *A Closer Look At the Target Malware, Part II*, Jan. 14, 2014, [www.krebsonsecurity.com/2014/01/a-closer-look-at-the-target-malware-part-ii/](http://www.krebsonsecurity.com/2014/01/a-closer-look-at-the-target-malware-part-ii/).

<sup>17</sup> Elizabeth A. Harris, Nicole Perlroth, Nathaniel Popper, and Hilary Stout, *A Sneaky Path Auto Target Customers' Wallets*, Jan. 17, 2014,

110. Other Target customers and shareholders learned of the massive data breach at Target stores on December 18, 2013, when KrebsOnSecurity.com, a website dedicated to reporting cybercrime, published an article about it. According to the site, Target was investigating the theft of millions of customer credit card records occurring in an "expanding window" of time just after Thanksgiving 2013. According to Krebs' post, one source stated that the breach would likely be one of the "largest retail breaches to date." Target had not responded to his multiple requests for comment.

111. By that point, Krebs had also spoken with a fraud analyst at a major bank who stated that his team had independently confirmed that Target had been breached before the Company spoke publicly. The analyst stated that his team saw a large chunk of stolen credit card data, based on cards tied to Target, for sale on an underground cybercrime forum. Krebs reported that the analyst stated more than one million cards were for sale, for anywhere between \$20 to \$100 per card.

**TARGET'S INITIAL DISCLOSURES ARE INADEQUATE AND UNDERSTATE  
THE SIZE OF THE BREACH**

112. Target did not discover the breach of its computer systems itself, only learning of it through the indirect effects of the breach. As CFO defendant Mulligan testified, on the evening of December 12, 2013, the U.S. Department of Justice ("DOJ") informed Target of suspicious activity involving payment cards used at its stores.<sup>18</sup>

---

[http://www.nytimes.com/2014/01/18/business/a-sneaky-path-into-target-customers-wallets.html?\\_r=0](http://www.nytimes.com/2014/01/18/business/a-sneaky-path-into-target-customers-wallets.html?_r=0).

<sup>18</sup> Mulligan Congressional Testimony.

Target met with the DOJ, the U.S. Secret Service, and a team of computer experts and, on December 15, 2013, finally confirmed that hackers had infiltrated the Company's systems, installed malware on its POS network, and stolen customer payment card data.

113. Despite being contacted by the DOJ, the most powerful law enforcement office in the country, defendant Mulligan and other Target executives failed to inform defendant Steinhafel of the data breach until Sunday, December 15, 2013. For the rest four days, the Individual Defendants remained silent despite knowing that customers had already suffered (and were continuing to suffer) fraudulent charges on their accounts.<sup>19</sup> After the fact, Target now claims it spent this time preparing to share accurate information with its customers about the breach. But, as shown below, Target understated the size of the breach in terms of both length of the breach and the number of customers impacted, and it delayed giving customers complete information. The inadequate disclosures aggravated the damage to affected customers.

114. Target attempted to remove the malware from its servers on December 15, 2013, but on December 18, 2013, it discovered that it had failed to remove the malware

---

<sup>19</sup> Almost all fifty states have security breach laws which impose requirements for informing customers upon a breach of a security system. *See, e.g.*, Minn. Statute 325E.61 (requiring disclosure "in the most expedient time possible and without unreasonable delay." SEC commissioner Aguilar has also addressed the importance of Board action immediately following a data breach, noting that companies "need to be prepared to respond within hours, if not minutes, of a cyber-event to detect the cyber-event, analyze the event, prevent further damage from being done, and prepare a response to the event." Luis A. Aguilar, *Cyber Risks and the Boardroom*, Conference New York Stock Exchange, June 10, 2014, [www.sec.gov/News/Speech/Detail/Speech/1370542057946#\\_ednref29](http://www.sec.gov/News/Speech/Detail/Speech/1370542057946#_ednref29).

on an additional twenty-five additional registers, and around "150 additional customers s accounts were affected."<sup>20</sup>

115. Once Krebs broke the report, Target could no longer remain silent. On December 19, 2013, a week after learning of the breach, and nearly a month after the breach commenced, Target disclosed incomplete information about the breach to its customers. Target acknowledged that "40 million credit and debit card accounts may have been impacted." Defendant Steinhafel stated he regretted the "inconvenience" the incident caused, but claimed Target places a "top priority" on protecting the security of its customers' personal information. On the same day, Molly Snyder, a Target spokeswoman, stated there was no indication that PINs were stolen.

116. The following day, December 20, 2013, defendant Steinhafel posted a message to Target costumers, discussing the stolen payment card data but claiming that there was no indication that PIN numbers were stolen. He acknowledged that Target (or the customers' banks) has responsibility for the fraudulent charges and thanked customers for their "understanding and loyalty" to Target. That same day, Target, at the direction and/or with the acquiescence of the Individual Defendants, issued a press release announcing that "the issue has been identified and eliminated" and that the Company would provide free credit monitoring services to affected customers. In an effort to

---

<sup>20</sup> Mulligan Congressional Testimony.

restore confidence in the Company, Target offered to extend its employees' discount of 10% to all customers who shopped in Target stores on December 21 and 22, 2013.

### **THE FULL SCOPE OF THE BREACH IS FINALLY REVEALED**

117. In an exclusive report, on December 24, 2013, *Reuters* stated that, despite prior statements by the defendants to the contrary, encrypted PIN data had, in fact, been stolen during the original breach.<sup>21</sup> The report cited a major bank that feared the thieves would be able to crack the codes and use them to make fraudulent withdrawals from the victims' bank accounts. The report also quoted a security expert who, noting the banks' unusual move of lowering withdrawal limits during the holiday season, believed that the bank had found data showing a vulnerability for cash withdrawals—something only possible with a customer's PIN. Furthermore, the report discussed the tools available to sophisticated cyber criminals, such as those that attacked Target, to decipher encrypted PINs.

118. The Individual Defendants were so ineffective and tardy in determining what was stolen from the Company's own systems that they did not learn what *Reuters* and banks knew until days after the information was reported. Target spokeswoman Molly Snyder responded to the *Reuters* report by e-mail, claiming that Target had "no reason to believe that PIN data, whether encrypted or unencrypted, was compromised."

---

<sup>21</sup> Jim Finkle and David Henry, *Exclusive: Target hackers stole encrypted bank PINs-source*, Dec. 24, 2013, [www.reuters.com/article/2013/12/24/us-target-databreach-Reuters/idUSBRE9BN0L220131224](http://www.reuters.com/article/2013/12/24/us-target-databreach-Reuters/idUSBRE9BN0L220131224).

Target posted data security updates on December 23 and 24, 2013, that still did not address the stolen PIN data.

119. On December 27, 2013, Target finally was forced to admit that customers' PIN data had been removed.<sup>22</sup> The Company admitted that it only learned of this on the morning of December 27, as a result of completion of additional forensics work. The Company claimed that the PIN data was strongly encrypted, but admitted that its external, independent payment processor could decrypt it. Now a month after the data breach began, the Individual Defendants were still trying to determine what was taken from Target's own systems, and were still contradicting the Company's earlier reports.

120. Even at this point, Target was still underestimating the size of the breach. On January 10, 2014, Target disclosed that *seventy million* customers had their personal information stolen during the breach.<sup>23</sup> These seventy million records were in addition to the forty million payment card records that Target had previously reported. The seventy million compromised records included names, mailing addresses, phone numbers, and e-mail addresses. In an insensitive understatement, defendant Steinhafel, the Company's CEO, admitted that it was "frustrating" for customers to learn about this, given that the compromised data could have been for sale on the Internet for nearly two months. By

---

<sup>22</sup> See *Target Data Security Media Update #4*, Dec. 27, 2013, <http://pressroom.target/news/target-data-security-media-update-4>.

<sup>23</sup> *Target Provides Update on Data Breach and Financial Performance*, Jan. 10, 2014, <http://pressroom.target.com/news/target-provides-update-on-data-breach-and-financial-performance>.

mid-January, with assistance from the DOJ, U.S. Secret Service, bank fraud analysts, *Reuters*, and newly hired forensic teams, the Individual Defendants finally were forced to take the blinders off, face the full scope of the theft that occurred on Target's own network, and admit that their failures were responsible for the harm now being suffered by Target.

121. Defendant Steinhafel sat for an interview with CNBC's Becky Quick in January 2014. "Clearly we're accountable ... and we're responsible," he acknowledged, referencing the holiday data breach.<sup>24</sup> "Liability is going to play out over time. *We know that from prior breaches*," he admitted.

122. On March 5, 2014, Target's then-CIO, defendant Jacob, "resigned." Target acknowledged that it needed to change its corporate governance, compliance, and risk practices. Before the breach, information security functions were split between various executives. The Company stated it would hire a CISO who would centralize those responsibilities. Target also stated its plans to separate one role for compliance with regulatory requirement and internal policies, and one for risk identification and risk monitoring.

---

<sup>24</sup> *CNBC Exclusive: CNBC Transcript: Target Chairman & CEO Gregg Steinhafel Speaks with Becky Quick Today on CNBC*, CNBC Business Day programming, Jan. 13, 2014.

123. Defendant Mulligan, Target's CFO at the time, testified before the U.S. Senate Committee on the Judiciary on February 4, 2014. He acknowledged that the Target only learned of the data breach upon being told by the DOJ.

124. On May 5, 2014, defendant Steinhafel "resigned" as the Company's CEO. The Board appointed defendant Mulligan to act as interim CEO and defendant Austin to act as interim Chair of the Board.

125. In response to the widespread governance and internal control failures that permitted the data breach to occur, a neutral and influential shareholder proxy advisor urged the ouster of most of Target's Board. On May 28, 2014, ISS recommended voting against seven Board members in light of their failure to manage risks and adequately protect the Company from data breaches. Specifically, ISS noted the failure of the Audit and Corporate Responsibility Committees, tasked with overseeing and managing risk, to manage data security risks that set the stage for the data breach. ISS further noted that Target's response to the breach, including replacing the CIO and improving security protocols, were "largely reactionary" and could have prevented the data breach had the Company implemented them sooner.

126. Target recognizes that its customers' personal and financial information is highly sensitive and must be protected. Indeed, Target promises its customers, in its Privacy Policy that it will "maintain administrative, technical and physical safeguards to protect [customers'] information" and "use industry standard methods to protect that information." Industry standard methods include the PCI DSS, which consists of twelve requirements, many of which were at issue in the data breach, including: (i) installing and



maintaining firewalls; (ii) changing vendor-supplied defaults for system passwords; (iii) using and regularly updating anti-virus software and programs; (iv) and tracking and monitoring all access to network resources and cardholder data.

127. On December 23, 2013, *USA Today* reported that Target likely was not complying with the PCI. The article stated:

Target's massive data breach took place just a few weeks before a set of payment card industry standards – known as PCI DSS 3.0 – were scheduled to go into effect. CyberTruth asked Nick Aceto, technology director at software vendor CardConnect, to supply some clarity.

CyberTruth: What does this latest databreach tell us about the efficacy of PCI?

Aceto: We can't say definitely that this breach is a failure of Target's PCI compliance, but *based on what Target has said, it's very hard to believe that they were even PCI 2.0 compliant at the time of the breach.*

A reason for thinking this is that the attack, involving an enormous amount of data, went on essentially unnoticed for 18 days. How were they not watching the network?

One of the PCI DSS requirements is that you monitor your logs and firewalls every day, looking for unusual activity. This monitoring involves file integrity checks and changes to critical systems files. What's more – the chapter 6 software development life cycle requires the secure distribution and verification of payment applications.

Unusual activity isn't always abnormal, but the point of PCI is to monitor and verify that all activity is normal, while not letting distractions – like busy shopping days Black Friday and Cyber Monday, on which the breach occurred – detract from the monitoring effort.

128. The Individual Defendants knew that the Company's less than industry-standard security systems and unreasonably vulnerable technologies would render its servers a target of hackers. The Individual Defendants, nonetheless failed to ensure that the Company took corrective measures to update its systems and technologies.

Among Target's deficiencies in this respect were its: failure to remedy known deficiencies in its POS system; failure to require two-factor identification and fully guard third-party access; failure to encrypt data and establish adequate firewalls to handle a server intrusion contingency; failure to monitor, respond to, and follow-up on security alerts; and failure to provide prompt and adequate warnings of security breaches. The Individual Defendants consciously disregarded their duties to ensure the implementation of, and to oversee and monitor, an adequate system of internal controls relating to data security and associated risks.

**THE INDIVIDUAL DEFENDANTS BREACHED THEIR FIDUCIARY DUTIES  
BY FAILING TO ESTABLISH AND MONITOR INFORMATION SECURITY  
CONTROLS**

129. As demonstrated above, the record-setting data breach occurred to Target because of a parade of failures by the Individual Defendants. Specifically, the Individual Defendants breached their fiduciary duty to Target by failing to implement and oversee adequate internal controls and governance with regard to data security, specifically through the following:

(a) failure to improve data security procedures and governance after the red flags of the 2009 breach, the data security warnings issued by Visa, Verizon, and various government agencies, and the known vulnerabilities in the POS system;

(b) failure to establish positions, with clear responsibility for data security, compliance with internal policies, and risk management such as a CISO, a CRO, and/or a Board member or committee;

(c) failure to nominate or elect Board members with a technical understanding of data security risks and/or the ability to oversee data security risk management and compliance programs;

(d) failure to limit the publication of excessive and unnecessary information about third-party vendors with access to vulnerable Target systems;

(e) failure to require two-factor authentication or otherwise limit to ensure the validity of third-party vendors seeking access to Target's systems;

(f) failure to employ firewalls and/or segregate or limit access to the areas of Target's system accessible by third parties to the areas of Target's system holding customers' personal and financial information;

(g) failure to enable the automatic deletion function for malware in the FireEye security program;

(h) failure to act on the first FireEye alert regarding malware upon notification from Bangalore, India;

(i) failure to act on the Symantec Endpoint Protection software alerts regarding malicious activity;

(j) failure to follow up on security alerts issued by FireEye and Symantec Endpoint Protection;

(k) failure to require proper elevation of security alerts to personnel enabled and authorized to take action to protect Target's system;

(l) failure to install personnel capable of recognizing and acting upon cyber attacks and threatened data breaches;

(m) failure to alter and/or eliminate default accounts per PCI DSS 2.1 and 11.5;

(n) failure to require "white listing" or otherwise permitting only approved processes to run on Target systems;

(o) failure to recognize and act upon the suspicious uploading from Target servers to Russian virtual private networks and otherwise monitor firewalls and logs;

(p) failure to act on the second FireEye alert regarding the exfiltration of data;

(q) failure to analyze the location of credentialed users in the network;

(r) failure to timely notify customers of the theft of their personal and financial information;

(s) failure to accurately notify customers regarding the scope and substance of the data breach; and

(t) failure to monitor cybercrime forums for fraudulent activity related to Target payment cards.

#### **DAMAGES TO TARGET**

130. As a result of the Individual Defendants' failures, thieves were able to steal 110 million records consisting of customers' sensitive personal and financial data. This failure to protect the Company's customers' personal and financial information has damaged its reputation with its customer base. In addition to price, Target's current and potential customers consider a company's ability to protect their personal and financial

information when choosing where to shop. Customers are less likely to shop at stores that cannot be trusted to safeguard their sensitive private information.

131. Further, as a direct and proximate result of the Individual Defendants' actions, Target has expended, and will continue to expend, significant sums of money. Such expenditures include, but are not limited to:

- (a) lost revenue and profits resulting from lost consumer confidence in Target's information security and the costs of restitution to customers affected by the breach;

- (b) costs associated with various investigations into the breach (e.g., the Company's internal investigation and investigations by the U.S. Secret Service and DOJ), including, but not limited to, expenses for legal, investigative, and consulting fees, and liability for any potential resulting fines or penalties;

- (c) increased cost of capital due to credit rating downgrades resulting from the breach;

- (d) costs incurred in connection with defending and paying any settlement or judgment in the class action cases filed by consumer plaintiffs and financial institution plaintiffs pending in this Court including, among other things, costs of notifying customers regarding replacing cards, sorting improper charges from legitimate charges, and reimbursing customers for improper charges; and costs associated with potential liability for non-compliance with PCI standards;

(e) costs related to remediation activities that were necessitated by the defendants' failure to promptly and sufficiently implement and remedy Target's inadequate information security systems and controls;

(f) lost revenue and profits resulting from Target's offer of a 10% discount to U.S. shoppers during the last weekend before Christmas 2013 in an effort to lure customers back into its stores; and

(g) costs incurred in connection with compensation and benefits paid to the Individual Defendants while they were breaching their fiduciary duties to Target, particularly defendant Steinhafel, who is eligible to receive approximately \$7 million in severance when his employment with Target is truly terminated.

#### **DERIVATIVE AND DEMAND FUTILITY ALLEGATIONS**

132. Plaintiffs bring this action derivatively in the right and for the benefit of Target to redress injuries suffered, and to be suffered, by Target as a direct result of breaches of fiduciary duty and waste of corporate assets, as well as the aiding and abetting thereof, by the Individual Defendants. Target is named as a nominal defendant solely in a derivative capacity. This is not a collusive action to confer jurisdiction on this Court that it would not otherwise have.

133. Plaintiffs will adequately and fairly represent the interests of Target in enforcing and prosecuting its rights.

134. Plaintiffs were shareholders of Target at the time of the wrongdoing complained of, have continuously been shareholders since that time, and are current Target shareholders.

135. At the time this action was commenced, Target's Board consisted of the following twelve individuals: defendants Austin, Baker, Darden, De Castro, Johnson, Minnick, Mulcahy, Rice, Salazar, Steinhafel, Stumpf, and Trujillo. Plaintiffs did not make any demand on the Board to institute this action because such a demand would be a futile, wasteful, and useless act for all of the reasons set forth below.

136. Plaintiffs also did not make any demand on the other shareholders of Target to institute this action since such demand would be a futile and useless act for at least the following reasons: (i) Target is a publicly held company with more than 633 million shares outstanding and thousands of shareholders; (ii) making a demand on such a number of shareholders would be impossible for plaintiffs who have no way of finding out the names, addresses, or phone numbers of shareholders; and (iii) making demand on all shareholders would force plaintiffs to incur excessive expenses, assuming all shareholders could be individually identified.

**The Board Faces a Substantial Likelihood of Liability for Consciously Disregarding Its Duties to Implement Adequate Internal Controls for Data Security and Risk Management Oversight**

137. All of the Board members are disqualified from fairly evaluating the derivative claims because they are responsible for damages suffered by Target as a result of the Company's massive data breach. The Board is and was responsible for implementing internal controls sufficient to protect Target customers' personal and financial information. Each member of the Board knew that proper cyber risk management procedures required substantial focused resources and dedicated personnel. The Board as a whole, and the Audit Committee in particular, were charged generally

with "Risk Assessment," but utterly failed to implement adequate internal controls to prevent the massive data breach that ultimately occurred.

138. The Board's failure of oversight reflects a conscious and deliberate disregard for their fiduciary duties—namely, inaction in the face of circumstances that plainly called for immediate action. As such, the Board faces a substantial likelihood of liability, rendering demand upon them futile.

139. As and as described above, the Board was aware of numerous facts reflecting serious deficiencies in Target's cybersecurity risk management practices. These facts include, but are not limited to, the following:

(a) Between 2005 and 2007, Target suffered a data breach stemming from its POS machines, which led to the loss of customers' personal and financial information;

(b) On August 27, 2007, Dr. Neal Krawetz, a data security expert working for Hacker Factor Solutions, publicly disclosed a White Paper titled "Point-of-Sale Vulnerabilities," which warned Target about the possibility of a POS data breach. The White Paper used Target as an example of the potential ramifications of a POS data breach at a major retailer and estimated that as many as fifty-eight million card accounts could be compromised if Target's POS system was compromised;

(c) Attacks like the one Target suffered were described and warned about in each year's version of the Verizon Data Breach Investigations Report; and



(d) In May 2013, the Department of Homeland Security issued a warning that it was "highly concerned about hostility against critical infrastructure organizations."

140. A majority of the Director Defendants also have had experiences with data breaches and cybersecurity risks by virtue of their service as executive officers, directors, or members of management in other companies. These experiences, which gave them additional insight into the importance of having robust cybersecurity risk management procedures, serve as additional red flags to these defendants and further render their failure to institute adequate procedures at Target a bad faith breach of their fiduciary duties:

(a) At times relevant hereto, defendant Steinhafel was a member of the Business Roundtable, and cybersecurity was a recurring topic during defendant Steinhafel's tenure there. Moreover, defendant Steinhafel was a member of the Retail Industry Leaders Association, which also has been extremely vocal on issues of cybersecurity;

(b) Defendant Johnson serves as a director of Goldman Sachs. On February 28, 2012, defendant Johnson signed a Goldman Sachs Annual Report on Form 10-K recognizing that cybersecurity was a "high priorit[y]" that required a complex set of principles, policies, and technology to protect its clients' and firm's assets;

(c) Defendant Trujillo is the former CEO of Telstra Corporation Limited, Australia's largest media and telecommunications company. Defendant Trujillo acknowledged the importance of cybersecurity, in a Report on Form 6-K, filed on June 4,

2007, stating that cybersecurity is "a big issue" and recognizing the need for firewalls, spam filters, and protection of network vulnerabilities. Defendant Trujillo has also been a director of The Western Union Company ("Western Union") since 2012. Western Union's Annual Report on Form 10-K filed on February 22, 2013, and signed by defendant Trujillo, specifically mentions of the dangers of cyber attacks and the importance of protecting against them;

(d) Defendant Mulcahy was a member of the Business Roundtable, where cybersecurity was a recurring topic and was elected its Chairman in February 2007. In September 2007, the Business Roundtable released an extensive report detailing the alarming risks posed to business and the U.S. economy in the chance of a major Internet disruption. The report, titled "Growing Business Dependence on the Internet: New Risks Require CEO Action," cites the potential widespread effects a cyber-disruption could have on society and urges CEOs to take necessary action to ensure continuity of their business. Defendant Mulcahy is also a director of LPL Financial Holdings Inc., where she signed the Annual Report on Form 10-K filed on February 26, 2013, that acknowledged the risks that a vulnerable information system pose to the company;

(e) Defendant Austin is a member of the American Institute of Certified Public Accountants, which frequently faced and discussed cybersecurity issues. Moreover, defendant Austin was a director of Teledyne Technologies Incorporated and signed the Annual Report on Form 10-K filed on February 26, 2013, which acknowledged the risks that a vulnerable information system posed to the company;

(f) Defendant Darden is a director of Cardinal Health, Inc. where he signed the Annual Report on Form 10-K filed on August 22, 2012, which acknowledged the risks that cybersecurity incidents and data breaches pose to the company;

(g) Defendant Rice is the CFO of Eli Lilly and Company and signed the Annual Report on Form 10-K filed on February 21, 2013, which acknowledged the size and complexity of its information technology systems, similar to Target's, made it "vulnerable to breakdown, malicious intrusion, and random attack";

(h) Defendant Stumpf is the Chairman and CEO of Wells Fargo & Company ("Wells Fargo"), one of the largest financial institutions in the world. As CEO and Chairman of Wells Fargo, defendant Stumpf signed the Annual Report on Form 10-K filed February 27, 2013, which acknowledged the importance of cyber attacks with regard to risk management and the substantial risk that cyber attacks pose to the company;

(i) Defendant Baker is a director of U.S. Bancorp, in which capacity he signed the Annual Report on Form 10-K filed on February 22, 2013, that recognized the difficulty of protecting its information security systems from cyber attack and the significant damage such an attack could cause on the company; and

(j) Defendant De Castro is the former Chief Operating Officer of Yahoo! Inc. ("Yahoo") and a former senior executive at Google Inc. ("Google"). In these positions, defendant De Castro understood the importance of having adequate processes and controls in a business that depends on Internet operations and online transactions in

light of breaches suffered by Yahoo! and Google in November 2013 and July 2012, respectively.

141. These ten Individual Defendants each knew the magnitude of damage that a data breach could cause and that robust corporate governance and risk management procedures were required and necessary to protect Target from being victimized by data hackers. Nonetheless, the Director Defendants failed to take any action in the face of numerous red flags showing the insufficient data security practices at the Company and failed to implement controls designed to protect against a data breach. Because of their failures to act in the face of a known duty to act to protect the Company, the Director Defendants face a substantial likelihood of liability, and demand against them would be futile.

**The Board Faces a Substantial Likelihood of Liability for Consciously Failing to Monitor Target's System of Internal Controls**

142. As to the modicum of internal controls concerning data security that Target did have in place, the Board consciously failed to monitor and respond to those controls. For example: (i) the Director Defendants permitted Target to turn off the auto-delete function of the FireEye program and failed to respond to the warnings generated by FireEye and Symantec Endpoint Protection; (ii) the Director Defendants failed to require the SOC personnel to follow-up on the FireEye and Symantec Endpoint Production warnings and failed to require compliance with PCI standards and other DSS best practices; (iii) the Director Defendants failed to require two-factor authentication, failed to remove default settings on Company software, and failed to follow industry best

practices with regard to data security; (iv) the Director Defendants did not ensure that Target had proper corporate governance and reporting structures in place, as shown by the decisions to fire the former CIO, to create a CISO position, and to restructure the risk management and compliance programs for data security; and (v) the Director Defendants failed to adjust Target's corporate governance to account for and oversee the growing risk of cyber attacks, a risk a majority of them recognized via their service on this Board and in external positions.

143. Due to their failure to create proper reporting structures, monitor necessary changes in corporate governance, and oversee the limited internal controls that were in place at Target in the face of numerous red flags, the entire Board faces a substantial likelihood of liability, and demand would thus be futile.

**The Board's Decision to Omit Information Regarding the True Nature and Extent of the Breach from Public Disclosure Was Not a Valid Exercise of Business Judgment**

144. The Board caused Target to disseminate false and misleading public statements concerning, among other things, the true nature and extent of the data breach at the Company. Consumers (and shareholders) were entitled to adequate and prompt notification about the data breach to help them mitigate the harm which might stem from the theft of their personal information. The Board, however, failed to take reasonable steps to have the Company notify consumers that their information had been compromised. The Company's public disclosures concerning the breach were improper, as discussed above, because: (i) they were untimely; (ii) they understated the scope of the

breach and those affected; and (iii) they diminished the severity of the harm to customers by failing to disclose that PINs were compromised.

145. The members of the Board knew (or were reckless in not knowing) that the improper statements did not timely, fairly, accurately, or truthfully convey the scope of the data breach. In addition, when deciding whether to approve statements to be publicly disseminated, each member of the Board was duty-bound to inform himself or herself of all reasonably-available information. Information concerning the true nature of the data breach was both reasonably available and material to members of the Board. The conduct described herein could not possibly be considered a valid exercise of business judgment. Accordingly, demand is excused.

146. The acts complained of constitute violations of the fiduciary duties owed by Target's officers and directors and these acts are incapable of ratification.

147. Target has been and will continue to be exposed to significant losses due to the wrongdoing complained of herein, yet the Individual Defendants and Board have not filed any lawsuits against themselves or others who were responsible for that wrongful conduct to attempt to recover for Target any part of the damages Target suffered and will suffer thereby.

148. In June 2014, the defendants appointed a Special Litigation Committee, effectively conceding that they are incapable of fairly and adequately investigating plaintiffs' claims; therefore demand as to them would be futile.

## COUNT I

### **Against the Individual Defendants for Breach of Fiduciary Duty**

149. Plaintiffs incorporate by reference and reallege each and every allegation contained above, as though fully set forth herein.

150. As alleged in detail herein, the Individual Defendants, by reason of their positions as officers and directors of Target and because of their ability to control the business and corporate affairs of Target, owed to Target fiduciary obligations of due care and loyalty, and were and are required to use their utmost ability to control and manage Target in a fair, just, honest, and equitable manner.

151. The Officer Defendants breached their duties of loyalty and care by knowingly and/or in conscious disregard of their fiduciary duties: (i) failing to implement a system of internal controls to protect customers' personal and financial information; (ii) failing to oversee the (inadequate) internal controls that failed to protect customers' personal and financial information; and (iii) causing and/or permitting the Company to conceal the full scope of the data breach, which led to the loss of 110 million records.

152. The Director Defendants breached their duty of loyalty by knowingly and/or in conscious disregard of their duties: (i) failing to implement a system of internal controls to protect customers' personal and financial information; (ii) failing to oversee the (inadequate) internal controls that failed to protect customers' personal and financial information; and (iii) causing and/or permitting the Company to conceal the full scope of the data breach, which led to the loss of 110 million records.

153. As a direct and proximate result of the Individual Defendants' breaches of their fiduciary obligations, Target has sustained significant damages, as alleged herein. As a result of the misconduct alleged herein, these defendants are liable to the Company.

154. Plaintiffs, on behalf of Target, have no adequate remedy at law.

## **COUNT II**

### **Against the Individual Defendants for Waste of Corporate Assets**

155. Plaintiffs incorporate by reference and reallege each and every allegation set forth above, as though fully set forth herein.

156. The wrongful conduct alleged includes the Individual Defendants' failure to implement adequate internal controls to detect and prevent the breach of the Company's customers' personal and financial information. Under the Individual Defendants' direction and purview, Target's customers became the victims of the second biggest data breach in retail history. The Company has already incurred substantial costs in investigating the data breach and cooperating with various government investigations. In addition, the Company lost revenue and profit due to its offer of a 10% discount to U.S. shoppers during the last weekend before Christmas 2013 in an effort to lure customers back into its stores after the data breach. The Company will continue to incur substantial costs from the numerous consumer class actions filed against it.

157. Further, the Individual Defendants caused Target to waste its assets by paying improper compensation and bonuses to certain of its executive officers and directors that breached their fiduciary duties.



158. As a result of the waste of corporate assets, the Individual Defendants are liable to the Company.

159. Plaintiffs, on behalf of Target, have no adequate remedy at law.

### **PRAYER FOR RELIEF**

WHEREFORE, Plaintiffs, on behalf of Target, demand judgment as follows:

A. Against the Individual Defendants and in favor of the Company for the amount of damages sustained by the Company as a result of the Individual Defendants' breach of fiduciary duty, waste of corporate assets, and aiding and abetting breaches of fiduciary duties;

B. Directing Target to take all necessary actions to reform and improve its corporate governance and internal procedures to comply with applicable laws and to protect the Company and its shareholders from a repeat of the damaging events described herein, including, but not limited to, putting forward for shareholder vote, resolutions for amendments to the Company's By-Laws or Articles of Incorporation, and taking such other action as may be necessary to place before shareholders for a vote of the following Corporate Governance Policies:

1. a proposal to strengthen the Company's controls over its customers' personal and financial information;

2. a proposal to create a committee specifically tasked with monitoring the Company's data security measures;

3. a proposal to establish new corporate governance and internal controls to enhance Board oversight of the protection of the Company's IT systems and data;

4. a proposal to establish new, full-time positions at the Company focused on improved data security and risk management procedures;

5. a proposal to establish new, full-time positions in the Company focused on compliance with the Company's data security and risk management best practices;

6. a proposal to strengthen the Company's disclosure controls; and

7. a proposal to strengthen the Board's supervision of operations and develop and implement procedures for greater shareholder input into the policies and guidelines of the Board.

C. Awarding to Target restitution from the Individual Defendants, and each of them, and ordering disgorgement of all profits, benefits, and other compensation obtained by the Individual Defendants;

D. Awarding Plaintiffs the costs and disbursements of this action, including reasonable attorneys' and experts' fees, costs and expenses; and

E. Granting such other and further equitable relief as this Court may deem just and proper.

### **JURY DEMAND**

Plaintiffs demand a trial by jury.

Dated: July 18, 2014

ROBBINS ARROYO LLP

/s/ Shane P. Sanders

---

SHANE P. SANDERS

Felipe J. Arroyo (admitted *pro hac vice*)

Shane P. Sanders (admitted *pro hac vice*)

Gina Stassi (admitted *pro hac vice*)

600 B. Street, Suite 1900

San Diego, CA 92101

Telephone: (619) 525-3990

Facsimile: (619) 525-3991

Email: farroyo@robbinsarroyo.com

ssanders@robbinsarroyo.com

gstassi@robbinsarroyo.com

*Lead Counsel for Plaintiffs*

VERIFICATION

I, Debra S. Goodman, hereby declare as follows:

I am an attorney with the Law Office of Debra S. Goodman P.C., counsel for Mary Davis. I have read the foregoing Consolidated Shareholder Derivative Complaint for Breach of Fiduciary Duty and Waste of Corporate Assets. I verify that the statements made in the foregoing Complaint are true and correct to the best of my knowledge information and belief.

I make this Verification because Mary Davis is absent from the County of Montgomery, where I maintain my office.

Executed this July 18, 2014, at Blue Bell, Pennsylvania.

  
DEBRA S. GOODMAN

VERIFICATION

I, Maureen Collier, hereby declare as follows:

I have read the Verified Consolidated Shareholder Derivative Complaint for Breach of Fiduciary Duty and Waste of Corporate Assets ("Consolidated Complaint"). Based upon discussions with and reliance upon my counsel, and as to those facts of which I have personal knowledge, the Consolidated Complaint is true and correct to the best of my knowledge, information, and belief.

I declare under penalty of perjury that the foregoing is true and correct.

Signed and Accepted:

Dated: 07/16/14

Maureen Collier

MAUREEN COLLIER

VERIFICATION

I, Shane P. Sanders, hereby declare as follows:

I am an attorney with Robbins Arroyo LLP, counsel for The Police Retirement System of St. Louis and lead counsel for plaintiffs in the consolidated shareholder derivative action. I have read the foregoing Consolidated Shareholder Derivative Complaint for Breach of Fiduciary Duty and Waste of Corporate Assets. I verify that the statements made in the foregoing Complaint are true and correct to the best of my knowledge, information, and belief.

I make this Verification because The Police Retirement System of St. Louis is absent from the County of San Diego, where I maintain my office.

Executed this July 18, 2014, at San Diego, California.

A handwritten signature in black ink, appearing to read 'SHANE P. SANDERS', written over a horizontal line.

SHANE P. SANDERS

STATE OF MINNESOTA

DISTRICT COURT

COUNTY OF HENNEPIN

FOURTH JUDICIAL DISTRICT

Case Type: Civil

---

BETH KOENEKE, Derivatively on  
Behalf of TARGET CORPORATION

Court File No:

v.

ROXANNE S. AUSTIN, DOUGLAS M.  
BAKER, JR., CALVIN DARDEN,  
HENRIQUE DE CASTRO, BETH M.  
JACOB, JAMES A. JOHNSON, MARY  
E. MINNICK, ANNE M. MULCAHY,  
DERICA W. RICE, KENNETH L.  
SALAZAR, GREGG W. STEINHAFEL,  
JOHN G. STUMPF and SOLOMON D.  
TRUJILLO,

**SHAREHOLDER DERIVATIVE  
COMPLAINT FOR BREACH OF  
FIDUCIARY DUTY AND WASTE OF  
CORPORATE ASSETS**

**JURY TRIAL DEMANDED**

Defendants,

and

TARGET CORPORATION, a Minnesota  
corporation,

Nominal Defendant.

---

Plaintiff Beth Koeneke, through her counsel, brings this action derivatively on behalf of nominal defendant Target Corporation ("Target" or the "Company") and alleges upon personal knowledge as to herself and her own acts, and as to all other matters based upon the investigation conducted by her counsel which included, among other things, analyst reports, news reports, press releases, and other publicly available information regarding the Company as follows:

1. This is a shareholder derivative action brought on behalf of the Company against the members of its Board of Directors and certain of its executive officers (“Independent Defendants” as defined below) seeking to remedy defendants’ breaches of fiduciary duties and other violations of the law.

2. Target is a retailing company operating throughout the United States and Canada with almost 2,000 store locations. It is headquartered in Minneapolis, Minnesota and its estimated annual sales exceed \$73.8 billion.

3. In November and December 2013, Target sustained one of the most massive security breaches in United States history. This security breach exposed Target’s customers’ confidential personal and financial information and data. This action arises out of the officers’ and directors’ responsibility for this security breach.

4. The security breach was first disclosed by the media on December 18, 2013. According to these initial reports, Target was investigating a major data breach potentially involving millions of credit and debit card records.

5. After widespread media coverage, in a press release on December 19, Target confirmed the breach, disclosing that it took place between November 27 and December 15. Target initially disclosed that up to 40 million customers’ credit and debit card accounts may have been compromised.

6. On December 27, Target disclosed that debit card PIN data also had been stolen, in encrypted form. On January 10, 2014, Target disclosed that the mailing addresses, phone numbers or email addresses of up to 70 million additional people also had been stolen, bringing the possible number of customers affected to up to 110 million.



Target also admitted that confidential information related not only to customers who had shopped at Target over the holiday but included other confidential customer information and data that Target had stored previously.

7. Target repeatedly delayed notifying consumers of the existence and magnitude of the security breach which began in November 2013 but was not fully disclosed until January 10, 2014.

8. Approximately 70 lawsuits have been filed throughout the country against Target, many as class actions. Many of the lawsuits have been brought by customers. Some of the financial institutions who must reissue cards have brought claims as well. These lawsuits typically are seeking damages as a result of Target's failure to adequately safeguard customer confidential information and related data and Target's failure to maintain adequate encryption, intrusion detection, and prevention procedures. Additional allegations based on Target's failure to properly notify customers are included in some of the complaints as well.

9. In addition, state attorney generals as well as federal authorities are investigating the security breach. The Federal Trade Commission ("FTC") has been asked by two U.S. Senators, Richard Blumenthal of Connecticut and Chuck Schumer of New York, to investigate the Target breach. Blumenthal wrote a letter to the FTC stating, "If Target failed to adequately protect customer information, it denied customers the protection that they rightly expect when a business collects their personal information....Its conduct would unfair and deceptive."

10. On January 17, 2014, *The New York Times* reported:

Target's system was particularly vulnerable to attack. It was remarkably open, experts say, which enabled hackers to wander from system to system, scooping up batches of information....With Secret Service agents in Minneapolis investigating the extent of the fraud, Javelin Strategy & Research, a consulting firm, estimates the total damage to banks and retailers could exceed \$18 billion. Consumers could be liable for more than \$4 billion in uncovered losses and other costs.

11. The Individual Defendants failure to implement and monitor appropriate safeguards to protect customer confidential information from theft and the Individual Defendants failure to timely and accurately report the data breach to its customers has caused damage to Target.

12. The conduct of the Individual Defendants constitutes a breach of fiduciary duties, gross waste of corporate assets, abuse of control and a violation of applicable legal standards governing their conduct.

13. Plaintiff brings this derivative action (a) to recover damages against Target's officers and directors for the benefit of the Company and (b) to require the Company to reform and improve its corporate governance and procedures to protect Target from repetitive instances of the damaging events described herein.

#### **JURISDICTION AND VENUE**

14. This Court has jurisdiction over this action pursuant to Minn. Stat. §543.19. The amount in controversy exceeds the jurisdictional minimum of this Court. Venue is proper under Minn. Stat. §542.09.

15. Target has a substantial presence in Hennepin County, and its principle executive offices are located at 1000 Nicollet Mall, Minneapolis, Minnesota. Each Individual Defendant has or had substantial and continuous contacts with Hennepin County

that make the exercise of personal jurisdiction over them proper. Certain of the defendants also live and are citizens of Minnesota.

#### **THE PARTIES**

16. Plaintiff Beth Koenke, was at all relevant times, a shareholder of Target and is a current Target shareholder.

17. Nominal defendant Target is a Minnesota corporation and its principal place of business is located in Minneapolis Minnesota. Target is named in this Complaint as a nominal defendant solely in a derivative capacity, and this shareholder derivative action is on its behalf.

18. Defendant Gregg W. Steinhafel is, and at all relevant times was, Target's President, Chief Executive Officer and Chairman of the Board. Steinhafel has been a director since 2007.

19. Defendant Roxanne S. Austin is, and at all relevant times was, a Target director and Chairman of Target's Audit Committee.

20. Defendant Douglas M. Baker, Jr. is, and at all relevant times was, a Target director and member of Target's Audit Committee.

21. Defendant Calvin Darden is, and at all relevant times was, a Target director and member of Target's Corporate Responsibility Committee.

22. Defendant Henrique De Castro is, and at all relevant times was, a Target director and member of Target's Corporate Responsibility Committee.

23. Defendant Beth M. Jacob is, and at all relevant times was, Target's Chief Information Officer, Executive Vice President, Target Technology Services.

24. Defendant James A. Johnson is, and at all relevant times was, Target's Lead Independent Director, a director and member of Target's Corporate Responsibility Committee.

25. Defendant Mary E. Minnick is, and at all relevant times was, a Target director and member of Target's Audit Committee and Corporate Responsibility Committee.

26. Defendant Anne M. Mulcahy is, and at all relevant times was, a Target director and member of Target's Audit Committee.

27. Defendant Derica W. Rice is, and at all relevant times was, a Target director and member of Target's Audit Committee.

28. Defendant Kenneth L. Salazar is, and at all relevant times was, a Target director and member of Target's Corporate Responsibility Committee.

29. Defendant John G. Stumpf is, and at all relevant times was, a Target director and member of Target's Audit Committee.

30. Defendant Solomon D. Trujillo is, and at all relevant times was, a Target director and Chairman of Target's Corporate Responsibility Committee.

31. Defendants, Austin, Baker, Darden, De Castro, Jacob, Johnson, Minnick, Mulcahy, Rice, Salazar, Steinhafel, Stumpf and Trujillo, are collectively referred to as "Individual Defendants."

#### **DUTIES OF INDIVIDUAL DEFENDANTS**

32. By reason of their positions as officers and/or directors of Target, and because of their ability to control the business and corporate affairs of Target, the Individual Defendants owed Target and its shareholders the fiduciary obligations of trust, loyalty, and

due care, and were and are required to use their utmost ability to control and manage Target in a fair, just and honest and equitable manner. The Individual Defendants were, and are required to act in furtherance of the best interests of Target and its shareholders so as to benefit all shareholders equally and not in furtherance of their personal interests or benefit.

33. Each director and officer of the Company owes to Target and its shareholders the fiduciary duty to exercise good faith and diligence in the administration of the affairs of the Company and in the use and preservation of its property and assets, and the highest obligations of fair dealing.

34. The Individual Defendants, because of their positions of control and authority as directors and/or officers of Target, were able to and did, directly and/or indirectly, exercise control over the wrongful acts complained of herein.

35. At all times relevant, each of the Individual Defendants was the agent of each of the other Individual Defendants and of Target and was at all times acting within the course and scope of such agency.

36. To discharge their duties, the officers and directors of Target were required to exercise reasonable and prudent supervision over the management, policies, practices and controls of the financial affairs of the Company. By virtue of such duties, the officers and directors were required to, among other things:

- a. Manage, conduct, supervise and direct the business affairs of Target in accordance with all applicable laws and industry standards;
- b. Neither violate, nor knowingly permit any officer, director, or employee of Target to violate applicable laws, rules, regulations and industry standards;

c. Establish and maintain security procedures and policies to ensure protection of customers' confidential personal and financial data

d. Establish and maintain systematic monitoring, internal controls and protocol of Target's security measures and to periodically investigate or cause independent investigation to be made of these systems and controls;

e. Establish and maintain procedures and policies to ensure that Target timely notifies its customers of any disclosure of their personal and financial data;

f. Remain informed regarding how Target carries out its security procedures, and upon receipt of notice or information of imprudent or unsound conditions or practices, to make reasonable inquiry in connection therewith, and to take steps to correct such conditions or practices; and

g. Conduct the affairs of Target in an efficient, business-like manner so as to make it possible to provide the highest quality performance of its business, to avoid wasting Target's assets, and to maximize the value of Target's stock.

37. Each Individual Defendant, by virtue of his or her position as a director and/or officer, owed to the Company and its shareholders the fiduciary duties of loyalty, good faith, the exercise of due care and diligence in the management and administration of the affairs of the Company, as well as in the use and preservation of its property and assets. The conduct of the Individual Defendants alleged herein involves a violation of their obligations as directors and/or officers of Target, the absence of good faith on their part, and a reckless disregard for their duties to the Company and its shareholders that the Individual

Defendants were aware, or should have been aware, posed a risk of serious injury to the Company.

38. The conduct of the Individual Defendants, who were also officers and/or directors of the Company, has been ratified by the remaining directors who collectively comprised all of Target's Board during the relevant time period.

39. The Individual Defendants, because of their positions of control and authority as officers and/or directors of Target were able to and did, directly and/or indirectly, exercise control over the wrongful acts complained of herein, and by failing to prevent employees and/or officers of the Company from engaging in such wrongful actions. In addition, the Company is now the subject of over 70 lawsuits including many class actions of state and federal regulatory investigations which necessitates the Company to incur excess costs arising from the Individual Defendants' wrongful course of conduct.

#### **CONSPIRACY, AIDING AND ABETTING AND CONCERTED ACTION**

40. In committing the wrongful acts alleged herein, the Individual Defendants have pursued, or joined in the pursuit of common course of conduct, and have acted in concert with and conspired with, one another in furtherance of their common plan or design. In addition to the wrongful conduct herein alleged as giving rise to primary liability, the Individual Defendants further aided and abetted and/or assisted each other in breach of their respective duties.

41. During all time relevant hereto, the Individual Defendants collectively and individually initiated a course of conduct that was designed to and did conceal that:

a. Individual Defendants failed to implement adequate internal controls relating to its security measures and protocol to protect its customers' personal and financial data; and

b. The Individual Defendants failed to timely and accurately inform customers regarding the scope and extent of the security breach.

42. In furtherance of this plan, conspiracy, and course of conduct, the Individual Defendants collectively and individually took the actions set forth herein.

43. The Individual Defendants engaged in a conspiracy, common enterprise, and/or common course of conduct. The Individual Defendants caused the Company to conceal the true facts regarding its deficient security measures, protocol and the security breach.

44. The purpose and effect of the Individual Defendants' conspiracy, common enterprise, and/or common course of conduct was, among other things: i) to disguise the Individual Defendants' breaches of fiduciary duty, abuse of control, and gross mismanagement, waste of corporate assets and (ii) to conceal adverse information concerning the security breach.

45. The Individual Defendants accomplished their conspiracy, common enterprise and/or common course of conduct by causing the Company to purposefully or recklessly implement inadequate security measures and protocol and to purposefully or recklessly conceal the scope and extent of the security breach from its customers. Because the actions described herein occurred under the authority of the Board, each of the Individual



Defendants was a direct, necessary and substantial participant in the conspiracy, common enterprise, and/or common course of conduct alleged herein.

46. Each of the Individual Defendants aided and abetted and rendered substantial assistance in the wrongs alleged herein. In taking such actions to substantially assist the commission of the wrongdoing alleged herein, each Individual Defendant acted with knowledge of the primary wrongdoing, substantially assisted in the accomplishment of that wrongdoing and was aware of his or her overall contribution to, and furtherance of, the wrongdoing.

#### **FACTUAL BACKGROUND**

47. Target, one of the largest discount retail stores in the United States, was subject to one of the most massive security breaches to its computer systems in history. Between November 27, 2013 and December 15, 2013, intruders gained access to Target's data network and stole the credit and debit card information for about 40 million Target customers and the personal information of 70 million customers.

48. Even though Target had knowledge of the security breach and was conducting an investigation, it did not initially make this information public. Instead, initial news reports on December 18, 2013 first disclosed the Target security breach.

49. On December 19, 2013, Target issued a press release which confirmed that it was aware of unauthorized access to payment card data. Target initially stated that its computer system had been compromised in all U.S. stores and that anyone who made credit or debit purchases from November 27, 2013 to December 15, 2013 had their names, credit and debit card numbers, the card's expiration date and the CVV code compromised.

50. On December 27, 2013, Target disclosed that there was unauthorized access to debit card PIN data as well. In its press release, Target stated that the PIN data was “strongly encrypted” and thus the debit cards were not compromised. There, however, remains a serious risk that the PIN data may be decrypted and fraudulently used.

51. On January 10, 2014, Target disclosed that “it has been determined that certain guest information—separate from the payment card data previously disclosed—was taken during the breach.” The stolen information includes names, mailing addresses, phone numbers and email addresses for up to 70 million customers nationwide.

52. The security breach could have been prevented. Security experts have indicated that Target’s security system was particularly inadequate. On January 17, 2014, *The New York Times* reported,

Entering through a digital gateway, the criminals discovered that Target’s systems were astonishingly open—lacking the virtual walls and motion detectors found in secure networks like many banks’. Without those safeguards, the thieves moved swiftly into the company’s computer servers containing Target’s customer data and to the crown jewel: the in-store systems where consumers swipe their credit and debit cards and enter their PINS.

53. More than one security expert has explained that Target’s data breach shows a security failure that should not have happened. Informationweek.com reported on December 21, 2013, that retailers who store credit card data are required to encrypt this data by the Payment Card Industry Data Security Standard. “If the data is properly encrypted...it shouldn’t be of any use to attackers.” In addition, it appears that Target violated the Standard by storing certain types of data which is not supposed to be stored at all. “The fact that three-digit CVV security codes were compromised shows they were

being stored. Storing CVV codes has long been banned by the card brands and the PCI [Security Standards Council].”

54. On December 23, 2013, USA Today also reported that Target was likely not compliant with the Standard. In addition, in 2007, Target was warned by a security expert about the possibility of this type of computer theft and the potential consequences of deficient security measures including the loss of millions of customers’ financial data. Target also was informed on how to prevent this type of attack.

55. The Individual Defendants knew or should have known that the Company did not have a sufficient security system in place to adequately secure and protect customers’ personal and financial information from theft, collection and misuse by third parties.

56. Already, over 70 civil lawsuits including many class actions have been filed against Target by its customers alleging a variety of state common law and statutory claims. In addition, class action lawsuits have been filed by financial institutions who have been forced to reissue cards and refund fraudulent purchases.

57. Reports of fraudulent card charges with credit cards used at Target have been growing since the Target security breach. According to one security expert, the type of data stolen from Target allows the creation of “counterfeit cards by encoding the information on any card with a magnetic stripe. If the thieves also were able to intercept PIN data for debit transactions, they would theoretically be able to reproduce stolen debit cards and use them to withdraw cash from ATMS.”

58. Target’s statement to consumers that the PIN data is safe has been questioned, *NPR* reported on December 29, 2013:

In a statement, Target says the stolen PINS were encrypted, so they're safe. They say the only people who could decrypt the PINs are at Target's external, independent payment processor. Stuart McClure, CEO of computer security company Cylance, isn't buying it. "To me, that's fantasy," McClure says. "I'm not quite sure what makes them think that." He says the stolen PIN data can be decrypted by the hackers. They can conduct what's called "brute-force decrypting" if they have the right tools and the time. "It just depends on how determined the adversary is, and how committed they are to performing the fraud," he says. "You're probably talking about weeks or months."

59. Security experts say that the confidential information stolen from Target will have a lasting effect on consumers. *The New York Times* reported, "'We're expecting this to be a major contributor, if not the primary driver of card fraud for the next 12 months,' said Alphonse R. Pascual, of Javelin Strategy & Research. 'Those cards will continue to have value for quite a while. These cards will still be available for purchase a year from now.'"

60. Security experts estimate that the damage from the Target breach to banks and other retailers could exceed \$18 billion and to consumers for uncovered losses and costs could exceed \$4 billion.

61. Computer security firm, Sophos, noted that "the average cost of a data breach in 2012 was \$188 per record in the U.S., including the cost of fines, legal damages and loss of business."

62. CBS News Minnesota reported that "Target is in a critical situation with consumers because its credibility and brand loyalty are being questioned....Target shoppers were scared off during the holiday season, when stores can make roughly 20 percent to 40 percent of their annual revenue."

63. Target recently announced that it now foresees fourth-quarter sales at stores open at least a year will be down about 2.5 percent. In addition, Target stated that its fourth-quarter financials may include charges related to the breach and that costs tied to the breach may have a material adverse effect on its quarterly results as well as future periods. Target said it is not able to estimate the costs, or range of costs, related to the data breach but said they may include liabilities to payment card networks for reimbursements of credit card fraud, card reissue costs and liabilities from civil litigation, government investigations and enforcement proceedings, expenses for legal, investigative and consulting fees, and incremental expenses and capital investments for remediation activities.

64. Several members of Congress have called for hearings into the Target breach while others have asked the FTC to investigate the breach and take appropriate action. Senator Blumenthal of Connecticut wrote to the FTC, "If Target failed to adequately and appropriately protect its customers' data, then the breach we saw this week was not just a breach of security, it was a breach of trust." Senator Franken of Minnesota stated that Target's security breaches "raise important questions about the responsibilities corporations have to protect consumers and inform their customers when data has been compromised."

65. The Attorney General from Minnesota said she was joining a nationwide investigation into Target's security breach. The joint probe includes over 30 state attorneys general. States have a variety of privacy laws to protect consumers from disclosure of their personal and financial data which may be utilized against Target.

66. As direct and proximate result of the Individual Defendants' wrongdoing, Target has and will continue to face significant losses and costs. These include, but are not

limited to, loss of revenue from a decline in shoppers visiting its stores, costs from the extensive civil litigation including class action lawsuits; costs from government investigations and enforcement proceedings, extensive expenses for legal, investigative and consulting fees; liabilities to payment card networks for reimbursements of credit card fraud; costs related to card reissuance; costs to provide free credit reports to its customers, and costs for remediation efforts.

#### **DERIVATIVE AND DEMAND FUTILITY ALLEGATIONS**

67. Plaintiff brings this action derivatively in the right and for the benefit of Target to redress injuries suffered, and to be suffered, by Target as a direct result of breaches of fiduciary duty, abuse of control, waste of corporate assets, and gross mismanagement, as well as the aiding and abetting thereof, by the Individual Defendants. Target is named as a nominal defendant solely in a derivative capacity. This is not a collusive action to confer jurisdiction on this Court that it would not otherwise have.

68. Plaintiff will adequately and fairly represent the interests of Target in enforcing and prosecuting its rights.

69. Plaintiff Beth Koeneke is a shareholder of Target at the time of the wrongdoing complained of, has continuously been a shareholder since that time, and is a current Target shareholder.

70. At the time this action was commenced, Target Board consisted of the following directors: Austin, Baker, Darden, De Castro, Johnson, Minnick, Mulcahy, Rice, Salazar, Steinhafel, Stumpf, and Trujillo.

71. As a result of the facts set forth herein, Plaintiff has not made any demand on the present Board to institute this action against the Individual Defendants. Such demand would be a futile and useless act, with respect to each and every one of the Individual Defendants because they are incapable of making an independent and disinterested decision to institute and vigorously prosecute this action for the following reasons:

a. Independent Defendants are disqualified from fairly evaluating the derivative claims, let alone vigorously prosecuting them, because they are each responsible for injuries suffered by Target as a result of security breach. The Board was responsible for implementing internal controls relating to its security measures and protocol to protect its customers' personal and financial data. Instead, the Board failed to implement sufficient internal controls to detect or prevent a data breach from occurring. The Individual Defendant failed to ensure that the Company implemented and maintained adequate safeguards to protect customers' personal and financial data. The Individual Defendants' wrongful conduct is a breach of their duty of loyalty. As such, the entire Board faces a substantial likelihood of liability; and

b. The Individual Defendants face a significant liability due to their failure to provide timely and adequate notice to consumers of the scope and extent of the security breach. The Individual Defendants breached their duty of loyalty by their causing the Company to delay disseminating accurate public statements as discussed herein. Accordingly, all the Board members face a substantial likelihood of liability;

c. Any suit by the current directors of Target to remedy these wrongs would expose Target to liability in the numerous pending consumer class actions lawsuits

and other litigation and regulatory investigations. There are currently over 70 lawsuits including many class action lawsuits filed against the Company as a result of the data breach. If the current directors were to bring this derivative action against themselves, they would thereby expose their own misconduct, which underlies allegations against them and which admissions would impair their defense of the pending litigation and regulatory investigations, in an amount likely to be in excess of any insurance coverage available to the Individual Defendants. Thus, the Individual Defendants would be forced to take positions contrary to the defenses they will likely assert.

72. The Individual Defendants wrongful acts constitute violations of the fiduciary duties owed by Target's officers and directors and these acts are incapable of ratification.

73. Target has been and will continue to be exposed to significant losses due to the wrongdoing complained of herein, yet the Individual Defendants and current Board have not filed any lawsuits against themselves or others who were responsible for that wrongful conduct to attempt to recover for Target any part of the damages Target suffered and will suffer thereby.

74. Plaintiff has not made any demand on the shareholders of Target to institute this action since such demand would be a futile and useless act for at least the following reasons:

a. Target is a publicly held company with over 632 million shares outstanding and thousands of shareholders;



b. Making demand on such a number of shareholders would be impossible for plaintiff who has no way of finding out the names, addresses, or phone numbers of shareholders; and

c. Making demand on all shareholders would force plaintiff to incur excessive expenses, assuming all shareholders could be individually identified.

75. Furthermore, the conduct complained of could not have been the product of good faith business judgment and thus the Individual Defendants are disqualified from fairly evaluating the derivative claims for the following reasons:

a. Each of these directors faces a substantial likelihood of liability in numerous civil lawsuits and regulatory investigations for breaching their fiduciary duties and other wrongdoing.

b. A derivative claim to recoup damages for harm caused to the Company by unlawful conduct represents a challenge to conduct that is outside the scope of the Board's business judgment—conduct for which the Board should face potential personal liability. Endangering customers' personal and financial data by failing to maintain proper security procedures and internal controls, and then failing to properly disclose the security breach to customers cannot be examples of legitimate business conduct. The protections of the business judgment rule do not extend to such malfeasance. Nor can such malfeasance ever constitute the good faith required of corporate fiduciaries;

c. As the ultimate decision-making body of the Company, the Board caused the Company to conceal and delay publication of accurate information regarding the scope and extent of the security breach. Each of the Individual Defendants knew or should

have known that the delayed and inaccurate statements did not timely, fairly or truthfully convey the scope and extent of the security breach. The Individual Defendants were bound by the duty of care to inform themselves of all reasonably-available material information about the security breach.

## COUNTS

### **FIRST CAUSE OF ACTION**

#### **Against Individual Defendants for Breach Of Fiduciary Duty**

76. Plaintiff incorporates by reference and realleges each and every allegation contained above, as though fully set forth herein.

77. As alleged in detail herein, the Individual Defendants, by reason of their positions as officers and directors of Target and because of their ability to control the business and corporate affairs of Target, owed to Target fiduciary obligations of due care and loyalty, and were and are required to use their utmost ability to control and manage Target in a fair, just, honest, and equitable manner.

78. The Individual Defendants breached their duty of loyalty by knowingly, recklessly, or with gross negligence: (i) failing to implement a system of security procedures, protocols and internal controls to protect customers' personal and financial information; and (ii) causing or allowing the Company to conceal the extent and scope of the security breach.

79. As a direct and proximate result of the Individual Defendants' breaches of their fiduciary obligations, Target has sustained significant damages, as alleged herein. As a result of the misconduct alleged herein, these defendants are liable to the Company.

80. Plaintiff, on behalf of Target, has no adequate remedy at law.

**SECOND CAUSE OF ACTION**

**Against Individual Defendants for Waste Of Corporate Assets**

81. Plaintiff incorporates by reference and realleges each and every allegation set forth above, as though fully set forth herein.

82. The wrongful conduct alleged included the failure to implement a system of security procedures, protocols and internal controls to protect customers' personal and financial information and also included the failure to implement adequate internal controls to detect and prevent the breach of the Company's customers' personal and financial information.

83. As a result of the misconduct described herein, which the Individual Defendants have caused, Target has and will continue to incur substantial losses and costs including but not limited to those related to defending over 70 lawsuits including class litigation, state and federal investigations and loss of customers.

84. The Individual Defendants also caused Target to waste its assets by paying improper compensation and bonuses to certain of its executive officers and directors that breached their fiduciary duty.

85. As a result of the waste of corporate assets, the Individual Defendants are liable to the Company.

86. Plaintiff, on behalf of Target, has no adequate remedy at law.

**THIRD CAUSE OF ACTION**

**Against Individual Defendants for Abuse Of Control**

87. Plaintiff incorporates by reference and realleges each and every allegation set forth above, as though fully set forth herein.

88. The Individual Defendants' misconduct alleged herein constituted an abuse of their ability to control and influence Target, for which they are legally responsible,

89. As a direct and proximate result of the Individual Defendants' abuse of control, Target has sustained significant damages.

90. As a result of the misconduct alleged herein, the Individual Defendants are liable to the Company.

91. Plaintiff on behalf of Target has no adequate remedy at law.

#### **PRAYER FOR RELIEF**

WHEREFORE, Plaintiff demands judgment as follows:

A. A determination and award to Target for the damages sustained by it as a result of the violations set forth above from each of the Individual Defendants;

B. A declaration that the Company must undertake necessary corrective actions to reform and improve its corporate governance and internal procedures to protect the Company from a repeat of the damaging events described in this Complaint, including but not limited to, adopting the following remedial measures:

1. Strengthening the Board's supervision through strong accountability measures to ensure that the Board implements proper controls and protocol over its security procedures;

2. Implementing corporate governance policies and committees to monitor and strengthen its security procedures;

3. Implementing corporate governance policies for increased shareholder participation; and

4. Adopting a process allowing the Company's shareholders to nominate at least three new candidates for election to the Board.

C. Ordering disgorgement of funds received by Individual Defendants based upon their misconduct alleged herein and awarding to Target restitution from the Individual Defendants;

D. Awarding plaintiff the costs and disbursements of this action, including reasonable attorneys' and experts' fees, costs and expenses; and

E. Granting such other and further equitable relief as this Court may deem just and proper.

**JURY DEMAND**

Plaintiff demands a trial by jury.

DATED: February 5, 2014

MYLES A. SCHNEIDER & ASSOC., LTD.

/s/ Myles A. Schneider  
MYLES A. SCHNEIDER (#305479)

710 DODGE AVENUE NW  
SUITE A  
ELK RIVER, MN 55330  
Telephone: 763-315-1100  
Facsimile: 877-294-4254

BONNETT, FAIRBOURN, FRIEDMAN  
& BALINT, P.C.  
ANDREW S. FRIEDMAN  
FRANCIS J. BALINT, JR.  
WENDY J. HARRISON  
2325 E. Camelback Rd., Suite 300  
Phoenix, Arizona 85012

Attorneys for Plaintiff



PENNSYLVANIA

22 CASSATT AVE.  
BERWYN, PA 19312  
TELEPHONE: (610) 225-2677  
FACSIMILE: (610) 408-8062

CALIFORNIA

12707 HIGH BLUFF DRIVE, SUITE 200  
SAN DIEGO, CA 92130  
TELEPHONE: (858) 794-1441  
FACSIMILE: (858) 794-1450

April 10, 2014

**VIA CERTIFIED MAIL**  
**RETURN RECEIPT REQUESTED**

Gregg W. Steinhafel  
Chairman of the Board, Chief Executive Officer and President  
Target Corporation  
1000 Nicollet Mall  
Minneapolis, MN 55403

**Re: Shareholder Demand Pursuant to Minn. R. Civ. P. 23.09**

Dear Mr. Steinhafel:

The undersigned firm represents the Paul Perry Revocable Living Trust (the "Stockholder"), a current holder of common stock of Target Corporation ("Target" or the "Company"). Pursuant to Minn. R. Civ. P. 23.09, we write on behalf of the Stockholder to demand that Target's Board of Directors (the "Board") take action to remedy breaches of fiduciary duties and/or violations of law by certain current and/or former directors and executive officers of the Company, including (but not necessarily limited to) yourself ("Steinhafel"), John J. Mulligan ("Mulligan"), Beth M. Jacob, James A. Johnson, Solomon D. Trujillo, Anne M. Mulcahy ("Mulcahy"), Roxanne S. Austin ("Austin"), Calvin Darden, Mary E. Minnick ("Minnick"), Derica W. Rice ("Rice"), John G. Stumpf, Douglas M. Baker, Jr., Henrique de Castro and Kenneth L. Salazar. Collectively, the foregoing executive officers and directors of the Company will be referred to herein as "Management."<sup>1</sup>

As you are aware, by reason of their positions as officers and directors of Target and because of their ability to control the business and corporate affairs of Target, Management owed and owes Target and its shareholders the fiduciary obligations of good faith, loyalty, and due

---

<sup>1</sup> This is particularly the case with respect to members of the Board's Audit Committee (the "Audit Committee"). Among other things, the members of the Audit Committee were charged with ensuring the Company's compliance with legal and regulatory requirements, with monitoring the Company's internal controls, and with overseeing the Company's risk management. At relevant times, Austin, Minnick, Rice and Mulcahy served as members of the Audit Committee.

care, and are required to use their utmost ability to control and manage the Company in a fair, just, honest, and equitable manner. The Stockholder believes that Management has violated these core fiduciary duty principles, causing Target to suffer damages. As set forth herein, these violations concern Management's responsibility for the second biggest data breach in retail history.

## **I. FACTUAL BACKGROUND**

### **A. Overview of the Company and its Privacy Policy**

According to its public filings, Target serves guests at 1,924 stores – 1,797 in the United States and 127 in Canada – and at Target.com. Target is the second largest general merchandise retailer in the United States.

As stated in the Company's own "Privacy Policy," Target routinely collects personal information from its customers, including a customer's name, mailing address, e-mail address, phone number, driver's license number, and credit/debit card number. In addition, when customers use their debit cards to make a purchase at Target, they are required to enter the PIN associated with their bank account. Target promises its customers that it will, among other things, "maintain administrative, technical and physical safeguards to protect your personal information. When we collect or transmit sensitive information such as a credit or debit card number, we use industry standard methods to protect that information."

### **B. Identity Theft**

Armed with a person's personal and financial information, identity thieves can encode the victim's account information onto a different card with a magnetic strip creating a counterfeit card that can be used to make fraudulent purchases. With the addition of a victim's PIN, a thief can use the counterfeit card to withdraw money from that person's bank account. Identity thieves can cause further damage to their victims by using personal information to open new credit and utility accounts, receive medical treatment on their health insurance, or even obtain a driver's license. Once a person's identity has been stolen, reporting, identifying, monitoring, and repairing the victim's credit is a cumbersome, expensive, and time-consuming process. In addition to the frustration of having to identify and close affected accounts and correct information in their credit reports, victims of identity theft often incur costs associated with defending themselves against civil litigation brought by creditors. Victims also suffer the burden of having difficulty obtaining new credit. Moreover, victims of identity theft must monitor their credit reports for future inaccuracies as fraudulent use of stolen personal information may persist for several years.

Monetary losses from identity theft total billions of dollars a year. As far back as 2008 (in a report published on October 21, 2008), The President's Identity Theft Task Force Report detailed the tremendous economic toll this type of theft takes on its victims. The significant impact identity theft can have on consumers, and the extreme financial ramifications the failure to secure personal information can cause, has led to the enactment of numerous privacy-related laws aimed toward protecting consumer information and disclosure requirements, including, for example: (i) Gramm-Leach-Bliley Act; (ii) Fair Credit Reporting Act; (iii) Fair and Accurate



Credit Transactions Act; (iv) Federal Trade Commission Act, 15 U.S.C. §§41-58; (v) Driver's Privacy Protection Act; (vi) Health Insurance Portability and Accountability Act; (vii) The Privacy Act of 1974; (viii) Social Security Act Amendments of 1990; (ix) E-Government Act of 2002; and (x) Federal Information Security Management Act of 2002.

Moreover, the recent wave of cyber-attacks striking American corporations prompted warnings from federal officials, including one issued in May 2013 by the Department of Homeland Security. In particular, the warning was issued by an agency called ICS-Cert, which monitors attacks on computer systems that run industrial processes. The warning stated that the government was "highly concerned about hostility against critical infrastructure organizations." In addition to the alerts from the government, Target and other retailers saw a significant uptick in malware trying to enter their systems in the year prior to the data breach.

Management was long ago notified of the risk of a potential data breach. On August 27, 2007, Dr. Neal Krawetz, a data security expert working for Hacker Factor Solutions, publicly disclosed a white paper titled "Point-of-Sale Vulnerabilities" (the "White Paper") that warned Target about the possibility of a point-of-sale data breach. The White Paper used Target as an example of the potential ramifications of a point-of-sale data breach at a major retailer and estimated that as many as fifty-eight million card accounts could be compromised if Target's point-of-sale system was compromised.

In addition to the warning in 2007, according to numerous reports, Target's computer security staff raised concerns about vulnerabilities in the Company's payment card system at least two months before the data breach. According to these reports, at least one analyst at the Company wanted to do a more thorough security review of its payment system—a request that was brushed off under Management's direction and on its watch.

Management was aware of the ramifications of failing to keep customers' data secure and knew that the Company could be subject to costly government enforcement actions and private litigation. As stated in the risk disclosures in the Company's Annual Report on Form 10-K filed with the U.S. Securities and Exchange Commission ("SEC") on March 20, 2013:

If we experience a significant data security breach or fail to detect and appropriately respond to a significant data security breach, we could be exposed to government enforcement actions and private litigation. In addition, our guests could lose confidence in our ability to protect their personal information, which could cause them to discontinue usage of REDcards, decline to use our pharmacy services, or stop shopping with us altogether. The loss of confidence from a significant data security breach involving team members could hurt our reputation, cause team member recruiting and retention challenges, increase our labor costs and affect how we operate our business.

### **C. The Breach**

Target's data breach, which began on November 27, 2013, compromised as many as 110 million customers' personal and financial data. Within days of the breach, millions of affected customers' financial and personal information was being sold on the black-market. Moreover,

bank cards that had only been used at Target were found to have been used to make unauthorized purchases at Target stores.

News of the data breach first broke out on December 18, 2013, when KrebsOnSecurity.com, a website dedicated to reporting cybercrime, published an article indicating the occurrence of a massive data breach at Target stores. According to the report, Target was investigating the possible theft of millions of customer credit card and debit card records beginning November 27, 2013, and extending as far as December 15, 2013. The breach was thought to have occurred when thieves accessed the Company's customers' personal and financial data by breaking into Target's point-of-sale system.

According to a report confirmed by Management, hackers first broke into Target's network in 2013 by stealing the login credential of a heating-and-air conditioning contractor. The contractor, Fazio Mechanical Services, has confirmed its login credential was breached. After entering through this Company vendor's connection, the hackers then moved laterally through Target's system, eventually accessing the system that handled payments at the Company's cash registers. There should not have been a route between a network for an outside contractor and the one for payment data.

Consumers were entitled to adequate and prompt notification about the data breach to help them mitigate the harm and avoid additional instances of fraud. Management, however, failed to take reasonable steps to notify consumers that their information had been compromised. In so doing, Management aggravated the damage to affected customers.

#### **D. The Disastrous Aftermath**

Only after news of the data breach spread did the Company (under Management's direction and on its watch) even mention the credit card database attack. On December 19, 2013, *over three weeks after the data breach began*, Management finally acknowledged the breach to the public. Management caused the Company to issue a brief statement in which it confirmed that it had been aware of unauthorized access to certain customers' credit and debit card data at the Company's U.S. stores. According to the statement, "[a]pproximately 40 million credit and debit card accounts may have been impacted between Nov. 27 and Dec. 15, 2013." In a separate statement issued that same day, Management conceded that customer data compromised in the data breach "included customer name, credit or debit card number, and the card's expiration date and CVV [card verification value]."

On December 20, 2013, in a rushed attempt to contain and minimize the perceived impact of the data breach, Management professed to "have worked swiftly to resolve the incident," and concluded that "there is no indication that PIN numbers have been compromised on affected bank issued PIN debit cards or Target debit cards." Management assured worried customers that "[s]omeone cannot visit an ATM with a fraudulent debit card and withdraw cash." That same day, Management issued a press release announcing that "the issue has been identified and eliminated" and that the Company would provide free credit monitoring services to affected

customers.<sup>2</sup> Moreover, in an effort to restore confidence in the Company, Target offered to extend its employees' discount of 10% to all customers who shopped in Target stores on December 21 and 22, 2013.

Despite Management's attempts to dispel customers' concerns, news began to emerge that credit and debit card information stolen from Target had begun to appear for sale online. According to an article by KrebsOnSecurity.com, customer account information stolen from Target was being sold on the black market "in batches of one million cards," and fraudulent purchase activity had begun being reported by issuing banks. As the growing scope of the breach continued to be revealed, Management confirmed on December 23, 2013, that the Secret Service and the United States Department of Justice ("DOJ") would investigate the breach. In addition, the Attorneys General from Massachusetts, New York, Connecticut, and South Dakota also began looking into the data breach (later to be joined by the Attorney General of Minnesota).<sup>3</sup> The following day, *Reuters* reported that, despite prior statements by Management to the contrary, encrypted PIN data had been stolen during the original breach, and those codes could be used by thieves to make fraudulent withdrawals from the victims' bank accounts. In response to these allegations, Management continued to deny that the PIN data of Target's customers had been compromised.

Indeed, Steinhafel sent a letter to Target's customers published shortly after the Company's initial acknowledgment of the breach which contended:

- That unauthorized access took place in U.S. Target stores between November 27 and December 15, 2013 and that Canadian stores and target.com were not affected.
- That "even if you shopped at Target during this time frame, it doesn't mean you are a victim of fraud. In fact, in other similar situations, there are typically low levels of actual fraud."
- There is no indication that PIN numbers have been compromised on affected bank issued PIN debit cards or Target debit cards. Someone cannot visit an ATM with a fraudulent debit card and withdraw cash.
- That "you will not be responsible for fraudulent charges—either your bank or Target have that responsibility."

However, on December 27, 2013, Management finally admitted that customers' PIN data had been compromised in the breach. Two weeks later, in yet another glaring indication that Management had not yet "resolved" the matter, Management released a statement indicating that the breach was far more significant than it had caused the Company to report. On January 10, 2014, Management disclosed that an additional **70 million** customers may have been affected by the data breach.

---

<sup>2</sup> Shortly after Target announced that it would provide free credit monitoring to customers, identity thieves began sending scam phishing e-mails to customers. These emails instructed the recipients to pass along their credit information so that it could be "monitored," when in fact it was being utilized for a fraudulent purpose.

<sup>3</sup> Upon information and belief, the joint probe now includes thirty states' attorneys general.

Several members of Congress have called for hearings into the Target breach, while others have asked the Federal Trade Commission (“FTC”) to investigate the breach and take appropriate action. On February 4, 2014, the Senate Judiciary Committee began to hold hearings on Target’s data breach and its potential impact on the Company’s customers. The Company’s Executive Vice President and Chief Financial Officer (“CFO”) Mulligan appeared before the Senate Judiciary Committee and expressed that Target was “deeply sorry” for losing its customers’ records to hackers. Mulligan stated that: “We will learn from this incident and, as a result, we hope to make Target, and our industry, more secure for customers in the future.” Also at the Senate Judiciary Committee hearing, Mulligan disclosed for the first time that Target found malware on twenty-five registers three days after the Company reported it had removed the threat from its system. As such, the data breach lasted until December 18, 2013, not December 15, 2013, as Management had previously reported.

The PCI Data Security Standard (“PCI”) is an industry standard for large retail institutions that accept credit card and debit card transactions. On December 23, 2013, *USA Today* reported that Target was likely not complying with the PCI. The article stated, in relevant part:

Target’s massive databreach took place just a few weeks before a set of payment card industry standards – known as PCI DSS 3.0 – were scheduled to go into effect. CyberTruth asked Nick Aceto, technology director at software vendor CardConnect, to supply some clarity.

CyberTruth: What does this latest databreach tell us about the efficacy of PCI?

Aceto: We can’t say definitely that this breach is a failure of Target’s PCI compliance, but based on what Target has said, it’s very hard to believe that they were even PCI 2.0 compliant at the time of the breach.

A reason for thinking this is that the attack, involving an enormous amount of data, went on essentially unnoticed for 18 days. How were they not watching the network?

One of the PCI DSS requirements is that you monitor your logs and firewalls every day, looking for unusual activity. This monitoring involves file integrity checks and changes to critical systems files. What’s more – the chapter 6 software development life cycle requires the secure distribution and verification of payment applications.

Unusual activity isn’t always abnormal, but the point of PCI is to monitor and verify that all activity is normal, while not letting distractions – like busy shopping days Black Friday and Cyber Monday, on which the breach occurred – detract from the monitoring effort.

Security experts have indicated that Target’s security system was particularly inadequate. On January 17, 2014, *The New York Times* reported:

Entering through a digital gateway, the criminals discovered that Target's systems were astonishingly open—lacking the virtual walls and motion detectors found in secure networks like many banks'. Without those safeguards, the thieves moved swiftly into the company's computer servers containing Target's customer data and to the crown jewel: the instore systems where consumers swipe their credit and debit cards and enter their PINS.

On March 13, 2014, *Reuters* published an article entitled "Target Missed Early Alert of Credit Card Data Breach: Report," which revealed that Management had been warned about a possible data breach on *November 30, 2013* (which is to say, weeks before Management revealed the attack). This article set forth, in relevant part:

*A Target Corp team of security experts, armed with a malware detection tool made by FireEye Inc, alerted company officials about a possible data breach on November 30, but they failed to respond to the warning signs, according to a media report on Thursday.*

The security specialists in Bangalore, India, monitoring computer logs found FireEye's alerts from November 30 and notified Target officials in Minneapolis, Bloomberg Businessweek reported. They also found more alerts from December 2, when more malware surfaced.

*Such warnings, if heeded, could have cut short the massive data breach that affected millions of customers who shopped at the nation's No. 3 retailer between November 27 and December 18 - the height of the U.S. holiday shopping season.*

Some 40 million credit and debit card records were stolen from the retailer, along with 70 million other records with customer information such as addresses and telephone numbers.

Congress is investigating the breach along with lapses that surfaced at other retailers, and credit card companies are pushing for better security.

\* \* \*

Bloomberg, citing a source who has consulted on the Target's investigation, said hackers deployed a custom-made code on November 30 that triggered a FireEye alert for the malware, including details on the servers where stolen data was to be delivered.

The security system's automatic function to delete such malware was turned off by Target's security team, the report said, citing two people who audited FireEye's role after the breach.

Target Chief Executive Gregg Steinhafel, in a statement to Bloomberg, said the retailer was still reviewing its “people, processes and technology” in the wake of the breach.

“As the investigation is not complete, we don’t believe it’s constructive to engage in speculation without the benefit of the final analysis,” Steinhafel wrote, according to the report.

He said the company had “already taken significant steps.” Target earlier this month said it was overhauling its information security practices.

Management was on notice that the Company’s less than industry-standard security systems and unreasonably vulnerable technologies would render its customers extremely vulnerable to attacks by third-parties. Management failed to take corrective measures to update its systems and technologies. Target’s deficiencies (under Management’s direction and on its watch) included the failure to maintain adequate backups and/or redundant systems, failure to encrypt data and establish adequate firewalls to handle a server intrusion contingency, and failure to provide prompt and adequate warnings of security breaches.

## **II. DEMAND PURSUANT TO MINN. R. CIV. P. 23.09**

Based on these events, the Stockholder contends that Management breached its fiduciary duties of loyalty and good faith by, among other things: (i) causing or allowing the Company to fall victim to the second largest data breach in retail history; (ii) consciously turning a blind eye to numerous red flags that arose in connection with the Company’s security systems; (iii) failing to provide adequate and prompt notice to consumers and conveying a false sense of security to Target customers affected by the breach; (iv) failing to establish and maintain adequate internal and financial controls; and (v) causing the Company’s financial statements to be materially false and misleading at all relevant times.

As a result, the Company has sustained damages, including (but in no way limited to): (1) the costs and potential fines associated with the investigations by the DOJ, state’s attorneys general and other entities; (2) the loss of customers (less likely to shop at Target due to lack of confidence that their personal information is safe); and (3) “meaningfully weaker-than-expected sales since the announcement,” which led Management to cut Target’s fourth quarter 2013 adjusted earnings per share (“EPS”) to between \$1.20 and \$1.30, compared to previous guidance of \$1.50 to \$1.60. Further, Management announced on January 22, 2014, that the Company was cutting health coverage for part-time workers as well as laying-off 475 workers and eliminating 700 open positions.

Accordingly, pursuant to Minn. R. Civ. P. 23.09, the Stockholder demands that the Board:


- (i) undertake (or cause to be undertaken) an independent internal investigation into the violations of Minnesota and/or federal law by each member of Management; and

- (ii) commence a civil action against each member of Management to recover for the benefit of the Company the amount of damages sustained by the Company as a result of their breaches of fiduciary duties and violations of Minnesota and/or federal law alleged herein.

If within a reasonable period of time after receipt of this letter the Board has not commenced an action and taken the other measures as demanded herein, the Stockholder will commence a shareholder's derivative action on behalf of the Company seeking appropriate relief.

Very truly yours,

THE WEISER LAW FIRM, P.C.

  
Robert B. Weiser

cc: Paul Perry Revocable Living Trust



WWW.WEISERLAWFIRM.COM

PENNSYLVANIA

22 CASSATT AVE.  
BERWYN, PA 19312  
TELEPHONE: (610) 225-2677  
FACSIMILE: (610) 408-8062

CALIFORNIA

12707 HIGH BLUFF DRIVE, SUITE 200  
SAN DIEGO, CA 92130  
TELEPHONE: (858) 794-1441  
FACSIMILE: (858) 794-1450

May 21, 2014

**VIA E-MAIL AND FIRST CLASS MAIL**

Wendy J. Wildung, Esq.  
Faegre Baker Daniels LLP  
2200 Wells Fargo Center  
90 South Seventh Street  
Minneapolis, MN 55402-3901

**Re: Shareholder Demand Pursuant to Minn. R. Civ. P. 23.09 by the Paul Perry  
Revocable Living Trust**

Dear Ms. Wildung:

Thank you for your letter dated May 2, 2014 acknowledging receipt of the demand pursuant to Minn. R. Civ. P. 23.09 (the "Demand") by the Paul Perry Revocable Living Trust (the "Stockholder") sent to the Board of Directors (the "Board") of Target Corporation ("Target") regarding the November 2013 data breach.

As you know, on May 6, 2014, it was announced that Gregg Steinhafel ("Steinhafel") had purportedly "resigned" as Target's President, CEO and Chairman. As set forth in the Demand, Steinhafel is one of the individuals who is alleged to have caused or allowed the Company to fall victim to the second largest data breach in retail history, and to have consciously turned a blind eye to numerous red flags that arose in connection with the Company's security systems

Among other things, the Company should not be obligated to provide any severance benefits whatsoever to Mr. Steinhafel in connection with his departure from the Company. To the extent that any such financial benefits have already been provided to Mr. Steinhafel, we hereby demand that these benefits be returned to the Company immediately. To the extent that no such benefits have been provided to date, we request that the Board enter into a "freeze" or standstill agreement with Mr. Steinhafel, holding any such benefits in abeyance during the investigation of this Demand and during the pendency of any action arising out of this Demand.

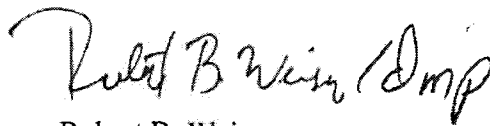


Wendy J. Wildung, Esq.  
May 21, 2014  
Page 2

Please indicate to us in writing whether Mr. Steinhafel and the Board are willing to enter into the "freeze" or standstill agreements described.

Thank you for your attention to this.

Very Truly Yours,

A handwritten signature in black ink, appearing to read "Robert B. Weiser". The signature is fluid and cursive, with the first name "Robert" and last name "Weiser" being more legible than the middle initial "B".

Robert B. Weiser

cc: Paul Perry Revocable Living Trust

# **APPENDIX B**

RESOLUTION APPOINTING SPECIAL  
LITIGATION COMMITTEE

WHEREAS, by letters dated April 10, 2014 and May 21, 2014, the Paul Perry Revocable Living Trust, a shareholder of the Company, made demand upon the Board of Directors to investigate and act upon certain potential legal claims belonging to the Company (all of them are the "Demand"); and

WHEREAS, the Company's counsel has explained that under the law governing Minnesota corporations, an appropriate response of the Board to the Demand is to form a special litigation committee consisting of one or more independent directors or other independent persons to consider the legal rights or remedies of the Company relating to the matters referenced in the Demand, and whether those rights or remedies should be pursued; and

WHEREAS, the Board wishes to form such a special litigation committee; and

WHEREAS, the Board has considered the information provided by Kathleen A. Blatz and John H. Matheson about their respective backgrounds, experience, and normal hourly billing rates; and

WHEREAS, the Board has been informed by the Company's counsel that Kathleen A. Blatz and John H. Matheson have been provided with information about the matters referenced in the Demand, including information about pending shareholder derivative complaints involving the same matters as the Demand, and that each of Kathleen A. Blatz and John H. Matheson has advised the Company's counsel that she/he does not have any personal interest in the subject matters of the Demand and does not know of any relationships or facts that would impair her/his willingness and ability to act independently on behalf of the Company in connection with such matters; and

WHEREAS, the Board has concluded that Kathleen A. Blatz and John H. Matheson have the requisite independence within the meaning of Section 302A.241 of the Minnesota Statutes to serve on a special litigation committee on behalf of the Company;

NOW, THEREFORE, BE IT RESOLVED, that pursuant to Section 302A.241 of the Minnesota Statutes, the Board does hereby form a Special Litigation Committee of the Board, and designate and appoint Kathleen A. Blatz and John H. Matheson as the two members of the Special Litigation Committee.

FURTHER RESOLVED, that the Special Litigation Committee is granted full power and authority: (1) to investigate the allegations, claims, and requests for relief set forth in the Demand, or otherwise raised by the Paul Perry Revocable Living Trust or other shareholders relating to the matters referenced in the Demand; (2) to determine whether and/or to what extent the Company should pursue whatever rights and remedies it has relating to such allegations, claims, and requests for relief; and (3) to respond on behalf of the Board and the Company to the Demand.

FURTHER RESOLVED, that the Special Litigation Committee is granted full power and authority to retain (1) special legal counsel who is independent of the Company and of the potential defendants identified in Demand to represent the Committee and advise it in its work, and (2) such other independent experts as the Committee deems necessary and appropriate in order to assist it in fulfilling its responsibilities. The expense of such counsel and/or experts shall be borne by the Company and/or its insurer.

FURTHER RESOLVED, that, in view of the substantial time and effort that is expected to be devoted by the members of the Special Litigation Committee in connection with performing their duties as such, each Committee member will be compensated by the Company and/or its insurer for the time expended by the member at such member's normal hourly rates.

FURTHER RESOLVED, that upon the completion of the Special Litigation Committee's work, the Committee is requested to inform the Board (1) that the Committee's work has concluded, and (2) of what response the Committee made to the Demand.

**SECOND BOARD RESOLUTION  
REGARDING SPECIAL LITIGATION COMMITTEE**

WHEREAS, by resolution adopted on June 11, 2014, the Board of Directors formed a Special Litigation Committee to consider a demand made by a shareholder of the Company upon the Board (the "Demand"); to investigate the matters raised by the Demand; to determine whether and/or to what extent the Company should pursue whatever rights and remedies it has relating to the allegations, claims, and requests for relief made in the Demand; and to respond on behalf of the Board and the Company to the Demand; and

WHEREAS, the Board appointed Kathleen A. Blatz and John H. Matheson as the two members of the Special Litigation Committee; and

WHEREAS, there are pending against the Company and against certain of its present and/or former officers and directors five shareholder derivative actions relating to the same matters as the Demand; and

WHEREAS, one of the shareholder derivative actions was brought by Beth Koeneke and is pending in the Hennepin County District Court, Minneapolis, Minnesota ("Hennepin County Action"); and

WHEREAS, four of the shareholder derivative actions were brought by Robert Kulla, Mary Davis, Maureen Collier, and The Police Retirement System of St. Louis, have been consolidated, and are pending in the United States District Court for the District of Minnesota ("Federal Actions"); and

WHEREAS, the Hennepin County Action and the Federal Actions (collectively, the "Litigation") relate to the same matters as the Demand, and involve similar allegations, claims, and requests for relief as the Demand; and

WHEREAS, the Board wishes the Special Litigation Committee to act on behalf of the Board and the Company with respect to the Litigation, as well as with respect to the Demand;

NOW, THEREFORE, BE IT RESOLVED, that in addition to the power and authority granted to the Special Litigation Committee on June 11, 2014, the Special Litigation Committee is granted full power and authority: (1) to investigate the allegations, claims, and requests for relief set forth in the Litigation, or otherwise raised by the plaintiffs in the Litigation, or raised by other shareholders in any derivative actions that might be filed in the future relating to the same matters as the Litigation ("Future Actions"); (2) to determine whether and/or to what extent the Company should pursue whatever rights and remedies it has relating to the allegations, claims, and requests for relief made in the Litigation or in any Future Actions; and (3) to respond on behalf of the Board and the Company to the Litigation and to any Future Actions.

# **APPENDIX C**

**GASKINS  
BENNETT  
BIRRELL  
SCHUPP**

STEVE GASKINS  
(612) 333-9503  
sgaskins@gaskinsbennett.com

July 24, 2014

Shane P. Sanders  
Robbins Arroyo LLP  
600 B St., Suite 1900  
San Diego, CA 92101

**Re: Davis, et al. v. Steinhafel, et al. v. Target Corporation**  
**(Lead Case No. 14-cv-00203-PAM-JJK)**  
**Special Litigation Committee of the Board of Directors of Target Corporation**

Dear Mr. Sanders:

We represent the Special Litigation Committee of Target's Board of Directors, which is investigating the allegations, claims, and requests for relief in the complaint you filed for the three shareholders derivatively on Target's behalf against certain of its current and former officers and directors. The SLC consists of two distinguished jurists, Chief Justice of the Minnesota Supreme Court (ret.) Kathleen Blatz and Professor John Matheson, who, before their appointment to the SLC, were not associated with Target.

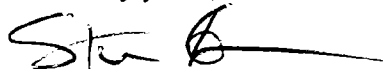
The investigation is in its beginning stage and the SLC would very much like to get your input on the issues raised in the consolidated complaint. Accordingly, the SLC has asked us to invite you to make a presentation on the issues arising from the allegations set forth in the demand, including your view of the factors bearing on whether there are rights and remedies Target has against the defendants named in the consolidated complaint that are in Target's best interests to pursue. The following dates and times are presently available:

Wednesday, July 30 at 2:00 pm  
Thursday, August 21 at 9:00 am  
Thursday, August 28 at 2:00 pm

Please let us know if one of these dates is convenient for you, and we will schedule your presentation. If not, please let us know and we will search for a mutually convenient alternative date.

If you have any questions or comments, or wish to set up a presentation, please feel free to call me or attorney Sara Daggett, who is fully familiar with this matter, at 612-333-9500.

Sincerely yours,



Steve Gaskins  
SWG/jt

**GASKINS  
BENNETT  
BIRRELL  
SCHUPP**

STEVE GASKINS  
(612) 333-9503  
sgaskins@gaskinsbennett.com

July 24, 2014

Myles A. Schneider, Esq.  
Myles A. Schneider & Assoc., Ltd.  
710 Dodge Avenue NW, Suite A  
Elk River, MN 55330

Andrew S. Friedman, Esq.  
Bonnett, Fairbourn, Friedman & Balint, P.C.  
2325 E. Camelback Rd., Suite 300  
Phoenix, AZ 85012

**Re: *Koenke, et al. v. Austin, et al. v. Target Corporation*, Case No. 27-cv-14-1832  
Special Litigation Committee of the Board of Directors of Target Corporation  
Our File No. 19767**

Dear Counsel:

We represent the Special Litigation Committee of Target's Board of Directors, which is investigating the allegations, claims and requests for relief in the complaint you filed for Ms. Koenke derivatively on Target's behalf against certain of its current and former officers and directors. The SLC consists of two distinguished jurists, Chief Justice of the Minnesota Supreme Court (ret.) Kathleen Blatz and Professor John Matheson, who, before their appointment to the SLC, were not associated with Target.

The investigation is in its beginning stage, and the SLC would very much like to get your input on the issues raised in the above-referenced complaint. Accordingly, the SLC has asked us to invite you to make a presentation on the issues arising from the allegations set forth in the complaint, including your view of the factors bearing on whether there are rights and remedies Target has against the defendants named in the complaint that are in Target's best interests to pursue. The following dates and times are presently available:

Wednesday, July 30 at 2:00 pm  
Thursday, August 21 at 9:00 am  
Thursday, August 28 at 2:00 pm

Please let us know if one of these dates is convenient for you, and we will schedule your presentation. If not, please let us know, and we will search for a mutually convenient alternative date.

If you have any questions or comments, or wish to set up a presentation, please feel free to call me or attorney Sara Daggett, who is fully familiar with this matter, at 612-333-9500.

Sincerely yours



Steve Gaskins  
SWG/jt



CC: SHD, SR, RWV


**BONNETT FAIRBOURN  
FRIEDMAN & BALINT PC**

WILLIAM G. FAIRBOURN  
VAN BUNCH  
ELAINE A. RYAN  
KATHRYN A. HONECKER  
GUY A. HANSON  
MANFRED P. MUECKE<sup>1</sup>  
T. BRENT JORDAN<sup>2</sup>  
LINDSEY M. GOMEZ-GRAY  
BARRETT N. LINDSEY

ANDREW S. FRIEDMAN  
ROBERT J. SPURLOCK  
WENDY J. HARRISON  
PATRICIA N. SYVERSON  
KIMBERLY C. PAGE  
WILLIAM F. KING  
ANDREW M. EVANS  
KEVIN R. HANGER  
KENDALL K. WILSON

FRANCIS J. BALINT, JR.  
C. KEVIN DYKSTRA  
ANDREW Q. EVERROAD  
JONATHAN S. WALLACK  
CHRISTINA L. BANNON  
TONNA K. FARRAR<sup>3</sup>  
TY D. FRANKEL  
ERIC D. ZARD

JERRY C. BONNETT, Of Counsel  
MICHAEL N. WIDENER, Of Counsel

<sup>1</sup> Admitted Only in California  
<sup>2</sup> Admitted Only in California, Kansas, Missouri  
and Oregon (located in Oregon)  
<sup>3</sup> Admitted Only in Pennsylvania

RECEIVED

AUG 13 2014

August 11, 2014

**VIA CERTIFIED MAIL****(RECEIPT NO. 7009 0080 0000 4081 6414 )**

Steve Gaskins  
Gaskins Bennett Birrell Schupp  
333 South Seventh Street, Suite 3000  
Minneapolis, MN 55402

Re: *Koeneke, et al. v. Austin, et al. v. Target Corporation, Case No. 27-cv-14-1832*

Dear Mr. Gaskins:

Thank you for your July 24, 2014 letter. We appreciate that you would like our input on the issues raised in the above-referenced complaint and that the SLC would like to meet with us.

As you are likely aware, there were also four shareholder derivative class action cases filed in federal court and, after consolidation, the Honorable Paul A. Magnuson appointed lead and liaison counsel for those actions.

We believe that it would be most appropriate to schedule a joint meeting that would include our firm, along with lead and liaison counsel for the federal actions.

If you have any questions or comments, please feel free to call me directly at 602.776.5902.

Very truly yours,

Andrew S. Friedman  
For the Firm

ASF:edz

## Stephanie J. Rubstello

---

**From:** Stephanie J. Rubstello  
**Sent:** Monday, August 25, 2014 1:45 PM  
**To:** 'afriedman@bffb.com'  
**Cc:** Steve W. Gaskins  
**Subject:** Target SLC Meeting

Dear Mr. Friedman,

I work with Steve Gaskins in representing Target's SLC for the recent data breach. I am following up on the telephone conversation you had with Mr. Gaskins last Friday in which you advised him that you would be willing to coordinate the state and federal court shareholder derivative plaintiffs' response to the SLC's invitation to meet with it. The SLC is interested in hearing the shareholders' perspectives in this case so I am writing to set up a time to meet.

The upcoming dates and times that work for the SLC are August 28<sup>th</sup> in the morning or afternoon, September 4<sup>th</sup> from 3pm to 5pm central time, and September 19<sup>th</sup> in the morning or afternoon. If none of those dates work for the plaintiffs please let us know and we can discuss dates for October.

Thank you,

Stephanie Rubstello

Stephanie J. Rubstello, Attorney  
Gaskins Bennett Birrell Schupp LLP  
333 South 7th Street, Suite 3000, Minneapolis, MN 55402-2440

[www.gaskinsbennett.com](http://www.gaskinsbennett.com)

[srubstello@gaskinsbennett.com](mailto:srubstello@gaskinsbennett.com)

TEL 612-333-9513 / FAX 612-333-9579

[My Bio](#)

[My V-Card](#)

[Map/Directions](#)

---

**CONFIDENTIALITY NOTICE:** This message contains confidential information intended for use of the named addressee(s) and may contain proprietary and/or legally privileged information. If you are not the designated recipient, you may not read, copy, distribute or retain this message. If you received this message in error, please notify the sender at (612) 333-9500, and destroy and delete it from your system. This message and any attachments are covered by the Electronic Communications Privacy Act, 18 U.S.C. §§ 2510-2521.

## Stephanie J. Rubstello

---

**From:** Shane P. Sanders <SSanders@robbinsarroyo.com>  
**Sent:** Thursday, August 28, 2014 4:40 PM  
**To:** Stephanie J. Rubstello; Steve W. Gaskins  
**Cc:** Gina Stassi  
**Subject:** Target shareholder derivative actions-meeting with SLC

**Follow Up Flag:** Follow up  
**Flag Status:** Flagged

Steve- It was nice chatting with you the other day. It appears that October 10 will work for both the federal and state derivative plaintiffs' counsel to meet with the SLC. Please confirm that date works on your end. Also, as I mentioned on our call, we intend to send you a letter in the next week or so that we believe will help the process along. Thank you and I look forward to discussing this matter with you further.

Shane P. Sanders  
Attorney at Law  
Robbins Arroyo LLP  
600 B Street, Suite 1900  
San Diego, CA 92101  
Telephone: (619) 525-3990  
Facsimile: (619) 525-3991  
Email: [SSanders@robbinsarroyo.com](mailto:SSanders@robbinsarroyo.com)  
[www.robbinsarroyo.com](http://www.robbinsarroyo.com)

This message and any attached documents contain information from the law firm of Robbins Arroyo LLP that may be privileged, confidential and/or exempt from disclosure under applicable law. If you are not the intended recipient, you may not read, copy, distribute or use this information. If you have received this email in error, please notify the sender and/or Robbins Arroyo LLP immediately by reply email and/or by telephone at (619) 525-3990 and delete this copy from your email system. Thank you.



Please consider the environment before printing this email.



600 B Street, Suite 1900  
San Diego, CA 92101  
619.525.3990 phone  
619.525.3991 fax  
www.robbsinarroyo.com

October 2, 2014

**VIA E-MAIL AND U.S. MAIL**

sgaskins@gaskinsbennett.com

Steve Gaskins, Esq.  
GASKINS BENNETT BIRRELL SCHUPP LLP  
333 South Seventh Street, Suite 3000  
Minneapolis, MN 55402

**Re: *Davis v. Steinhafel, et al.*, Lead Case No. 14-cv-00203-PAM-JJK  
Special Litigation Committee of the Board of Directors of Target  
Corporation**

Dear Mr. Gaskins:

I write regarding our forthcoming meeting with the Special Litigation Committee ("SLC") of Target Corporation's Board of Directors (the "Board"), tentatively scheduled for October 10, 2014. We appreciate the SLC's invitation to provide input regarding the issues raised in the consolidated complaint and look forward to this important opportunity to serve our clients' and the company's interests. As discussed, we have prepared a written submission to the SLC, which we hope will provide a meaningful framework for our discussions, attached hereto as Schedule A. We look forward to a productive meeting with the SLC on October 10 (or a mutually agreed-upon date thereafter).

Sincerely,

A handwritten signature in black ink, appearing to read 'Shane P. Sanders', is written over a horizontal line. The signature is fluid and cursive, with a long, sweeping underline that extends to the right.

Shane P. Sanders, Esq.

cc: Felipe J. Arroyo, Esq. (via email only)  
Gina Stassi, Esq. (via email only)  
Daniel L. Sachs, Esq. (via email only)  
Andrew S. Friedman, Esq. (via email only)  
Eric Zard, Esq. (via email only)

## SCHEDULE A

### **I. SUMMARY OF PLAINTIFFS' CONCERNS**

The data security breach at Target Corporation ("Target" or the "Company") in late 2013 caused the Company to suffer substantial monetary damages and significant reputational harm.<sup>1</sup> Plaintiffs believe it is critical for the Special Litigation Committee's ("SLC") investigation to focus on the nature and extent of these damages, to identify the individuals responsible for causing these damages, and to determine the most effective means to address and remedy the harm that these individuals' actions and inaction have caused to Target.

### **II. DAMAGES TO TARGET**

In evaluating whether Target should seek a monetary recovery from those individuals responsible for the damages to the Company, the SLC should conduct a detailed evaluation of the damages Target has suffered as a result of the 2013 data breach. At a minimum, the SLC should evaluate the following categories of damages: (1) costs directly associated with the data breach; (2) lost revenue and profits resulting from diminished consumer confidence in Target's information security; (3) costs incurred in connection with government investigations; (4) costs associated with the class actions pending against Target; (5) increased cost of capital due to credit rating downgrades resulting from the breach; and (6) costs incurred in connection with compensation and severance benefits improperly paid to defendant Steinhafel. ¶¶7, 130-31.<sup>2</sup>

#### **A. Costs Directly Associated With the Data Breach**

As of August 2, 2014, Target had spent a total of \$236 million on data breach related expenses, offset by a \$90 million insurance receivable, for a net of \$146 million.<sup>3</sup> These expenses include costs related to the Company's internal investigation, additional call center

---

<sup>1</sup> See generally plaintiffs' Verified Consolidated Shareholder Derivative Complaint ("Complaint") filed on July 18, 2014.

<sup>2</sup> All paragraph references ("¶\_\_" or "¶¶ \_\_") are to the Complaint.

<sup>3</sup> Target Form 10-Q, filed August 27, 2014.

staffing, legal and professional fees, and compensation to payment card networks for fraud losses. Target representatives have acknowledged that the Company will continue to incur legal, consulting, and administrative costs related to the data breach.<sup>4</sup> The Ponemon Institute, a data security research firm, estimates that the average per capita cost of a data breach is \$201 for U.S. companies, which would put the total cost of the Target data breach of 110 million records at approximately \$22 billion.<sup>5</sup>

#### **B. Lost Revenue and Profits Due to Reputational Harm**

Target has also suffered harm to the Company's reputation as a result of the data breach. For example, after announcing the data breach in December 2013, Target experienced a 46% drop in net profit.<sup>6</sup> The damage to the Company's reputation has extended far beyond this immediate harm, however. During the Company's 2Q 2014 earnings call on August 20, 2014, CFO John Mulligan ("Mulligan") noted that the Company has "seen a slower trend in debit card applications since the data breach, which is leading to slower growth in sales penetration."<sup>7</sup> The SLC should evaluate whether and to what extent losses in Target's revenue and profits are attributable to the reputational harm caused by the data breach.

#### **C. Government Investigations**

Since the December 2013 data breach, the U.S. Department of Justice, Secret Service, Federal Trade Commission, and the law enforcement agencies of several states have commenced investigations into Target's information security systems. In addition to the legal and

---

<sup>4</sup> In providing its third-quarter and full-year earnings guidance for 2014, Target did not include potential additional costs related to the data breach beyond what it has already recognized, which Target CFO defendant John Mulligan ("Mulligan") acknowledged "are not estimable" during the Company's 2Q 2014 earnings call held August 20, 2014.

<sup>5</sup> Ponemon Inst., *2014 Cost of Data Breach Study: United States* (May 2014).

<sup>6</sup> See Target Press Release, February 26, 2014, *Target Reports Fourth Quarter and Full-Year 2013 Earnings*.

<sup>7</sup> Mulligan, 2Q 2014 earnings call held August 20, 2014.

investigatory expenses described above, Target may incur substantial costs for potential fines and penalties if these investigations reveal violations of law.

#### **D. Related Class Actions**

Target may also incur substantial additional costs in connection with any settlement or judgment in the class actions brought against the Company as a result of the breach. Various financial institutions have alleged that they sustained millions of dollars of damages associated with the costs of notifying their customers, replacing cards, sorting improper charges from legitimate charges, and reimbursing customers for improper charges. Target consumers have also asserted claims against the Company for violations of state consumer protection acts and data breach statutes, violations of the Federal Stored Communications Act, and negligence, fraud, breach of contract, unjust enrichment, bailment, conversion, and invasion of privacy.

#### **E. Increased Cost of Capital**

Target's cost of capital is likely to increase as a result of the data breach—in fact, defendant Mulligan recently acknowledged that the Company's "business performance is not where it needs to be to sustain our middle A credit ratings."<sup>8</sup>

#### **F. Compensation and Severance Benefits Paid to Defendant Steinhafel**

When defendant Gregg Steinhafel ("Steinhafel") "resigned" in May 2014, the Board permitted him to remain employed by Target in an "advisory capacity," earning the same salary as when he was the Company's CEO, and he remains eligible for a fiscal 2014 short-term incentive payout opportunity under Target's Short-Term Incentive Plan.<sup>9</sup> Defendant Steinhafel is also eligible to receive severance benefits worth approximately \$7 million when his employment at the Company is finally terminated.<sup>10</sup>

---

<sup>8</sup> Mulligan, 2Q 2014 earnings call held August 20, 2014.

<sup>9</sup> See Target Form 10-Q, filed August 27, 2014, Ex. (10)AA.

<sup>10</sup> See Target DEFA-14A, filed May 27, 2014.

### III. INDIVIDUALS RESPONSIBLE FOR CAUSING DAMAGE TO TARGET

In identifying the individuals who are responsible for the damages Target suffered as a result of the 2013 data breach, the SLC should consider both the events leading up to the breach and the Company's responses to the breach. Upon its evaluation of these issues, described in further detail below, the SLC should determine whether the Company should pursue any of the claims asserted derivatively by Plaintiffs and whether it is necessary to commence additional legal proceedings in order to seek recovery from those individuals that are responsible for the damages to Target.<sup>11</sup>

#### A. Events Leading Up to the December 2013 Data Breach

Many of the Individual Defendants<sup>12</sup> knew that Target's point-of-sale ("POS") machines were vulnerable to similar data breaches due to previous attacks on the Company's computer network in 2005 and 2007. ¶¶2, 50-51, 121. Target executives and directors also received several other warnings about data security risks in recent years. ¶¶3, 52-59. Furthermore, many members of Target's Board have relevant experience at other companies and professional organizations such that they should have been aware of: (1) the importance of sound cybersecurity practices; and (2) the likelihood that Target would suffer significant damages from potential breaches of the Company's information security systems. *See, e.g.*, ¶140(a)-(j). In evaluating the Individual Defendants' liability for oversight lapses that led to the data breach, the SLC should consider, among other things, the Individual Defendants' response to the attacks on the Company's computer networks in 2005 and 2007 and their knowledge of the risks posed by future similar attacks.

---

<sup>11</sup> The SLC also should evaluate whether it is necessary to obtain tolling agreements from any individuals other than the Individual Defendants.

<sup>12</sup> "Individual Defendants" refers to Steinhafel, Beth M. Jacob ("Jacob"), James A. Johnson, Mulligan, Anne M. Mulcahy, Roxanne S. Austin, Calvin Darden, Mary E. Minnick, Derica W. Rice, John G. Stumpf, Douglas M. Baker, Jr., Henrique De Castro, Kenneth L. Salazar, and Solomon D. Trujillo.



The SLC also should take into consideration how other companies have responded to similar attacks. For example, between 2005 and 2007, The TJX Companies ("TJX") was hacked by the Alberto Gonzalez criminal consortium<sup>13</sup>—the same group responsible for the 2005 and 2007 attacks at Target. *See* ¶¶50-51. TJX subsequently charged its audit committee with, among other things, responsibility for overseeing the security of the company's computer system with respect to customer data, including compliance with the Payment Card Industry Data Security Standards.<sup>14</sup> Additionally, JPMorgan & Co. ("JPMorgan") has acknowledged that it regularly suffers denial-of-service attacks and data breach attacks from technically sophisticated and well-resourced criminals.<sup>15</sup> In response, JPMorgan's board and audit committee have taken steps to become regularly informed as to the company's cybersecurity policies and practices, as well as significant cybersecurity events.<sup>16</sup>

Further, the SLC should consider whether the Company's internal reporting systems and controls were sufficient to enable upper-level management and the Board to be adequately informed of risks and vulnerabilities in Target's information security systems in the months leading up to the December 2013 data breach. *Bloomberg* reported, based upon interviews with at least ten former Target employees familiar with the Company's data security operations, that management was alerted to the risks Target's lax oversight posed to the Company in the weeks leading up to the breach. ¶4. *Bloomberg* also reported that the Individual Defendants were not aware of the data breach until they were informed by the U.S. Secret Service. *Id.*

Finally, in order to adequately evaluate the Individual Defendants' liability and identify additional individuals that are responsible for the damages Target sustained as a result of the data

---

<sup>13</sup> *See* Louisiana Municipal Police Employees' Retirement System v. Alvarez, C.A. No. 5620 (Del. Ch. July 2, 2010).

<sup>14</sup> *Id.*

<sup>15</sup> *See* JPMorgan Form 10-Q August 4, 2014, at 73.

<sup>16</sup> *Id.*

breach, the SLC should assess Target's information security systems and cybersecurity risk management practices, overall. At a minimum, the SLC should ask the following questions during witness interviews:<sup>17</sup>

- What remedial measures were taken at Target in response to the 2005 and 2007 cyber attacks? By whom? Did the Board conduct any investigation or audit of the efficacy of these remedial measures?
- How often did the Board discuss or evaluate Target's information security systems and cybersecurity risk management practices? What information did the Board receive regarding these issues and from whom? How did the Board respond to this information? Did the Board obtain any opinions from third-party advisors regarding these issues?
- Who was responsible for determining what amount of resources Target allocated toward information security and cybersecurity risk management in 2013? What percentage of the Company's overall resources did this comprise? Did any of the Individual Defendants review or approve this resource allocation?
- Were members of Target's information protection team aware of vulnerabilities or risks posed by the POS systems utilized in Target's U.S. and Canadian stores? What was the nature of these risks?
- Did the Individual Defendants or senior management receive any reports (written or oral) regarding deficiencies in the Company's information security systems, including vulnerabilities or risks posed by the POS systems utilized in Target's U.S. and Canadian stores? What was the content of these reports? Who received these reports, when, and from whom? How did the individuals who received these reports respond?
- What policies and procedures were in place for monitoring Target's compliance with the Payment Card Industry Security Standards Council ("PCISSC") framework? Who was responsible for overseeing the Company's response to any reports of noncompliance? Did any of the Individual Defendants review or approve any policies, procedures, personnel, or allocation of resources relating to Target's compliance with the PCISSC framework?
- Who was responsible for selecting the cyber security products or platforms provided by FireEye or Symantec? Who was responsible for monitoring alerts from FireEye and Symantec? What policies, procedures, or protocols were in

---

<sup>17</sup> The SLC should, of course, develop additional questions based upon the information that is obtained during the course of the witness interviews and the SLC's investigation, overall.

place for responding to those alerts? Who was responsible for establishing these policies, procedures, or protocols? Did any of the Individual Defendants review or approve any policies, procedures, personnel, or allocation of resources relating to the monitoring of alerts from FireEye and Symantec?

- What policies and procedures were in place to ensure the secure exchange of information with third party contractors and any party, software or hardware connected to the Target network, and the IT security requirements for any party, software or hardware connected to the Target network? Who was responsible for overseeing these policies and procedures? Did any of the Individual Defendants review or approve any of these policies or procedures?
- What policies and procedures were in place to ensure the security of accounts connected to Target's network, specifically default accounts? Did Target personnel consider requiring two-factor identification for third parties? Who was responsible for overseeing and developing the policies and procedures relating to default accounts? Did any of the Individual Defendants review or approve any of these policies or procedures?
- What was the effect of the departure of Brian Bobo, Target's former Security Operations Center manager?
- What policies and technologies were in place to monitor and report suspicious data transmissions and/or so called "white listing" within Target's network? Who was responsible for overseeing the Company's response to any reports of suspicious data transmissions and/or so called "white listing" within Target's network? Did any of the Individual Defendants review or approve any policies, technology, personnel, or allocation of resources relating to the monitoring and reporting of suspicious data transmissions or the Company's response to reports of suspicious data transmissions?
- What policies and technologies were in place to monitor "firewall" and/or the freedom of movement within Target's network? Did any of the Individual Defendants review or approve any policies, technology, personnel, or allocation of resources relating to monitoring "firewall" and/or the freedom of movement within Target's network?
- What policies and technologies were in place to monitor fraudulent debit/credit or Target card activity? Who was responsible for overseeing the Company's response to any reports of potentially fraudulent card activity? Who was responsible for overseeing the Company's response to any reports of potentially fraudulent card activity? Did any of the Individual Defendants review or approve any policies, technology, personnel, or allocation of resources relating to the monitoring and reporting of potentially fraudulent card activity or the Company's response to reports of potentially fraudulent card activity?

- Who was responsible for developing, implementing, and overseeing Target's information security systems and cybersecurity risk management procedures that were in place in November 2013?
- Who received alerts from FireEye and Symantec in November or December of 2013? What procedures were in place for reporting these alerts to upper-level management and/or the Board? Did any of the Individual Defendants or senior management receive any reports (written or oral) regarding alerts from FireEye and Symantec in November or December of 2013?
- When and how did each of the Individual Defendants learn of the December 2013 data breach?

#### **B. Response to the Data Breach**

Target's disclosures immediately following the data breach understated the size of the breach and misleadingly represented to customers that no PIN data was compromised. ¶¶114-20. In determining whether the Individual Defendants' response to the data breach was consistent with their fiduciary duties owed to the Company, the SLC should evaluate whether Target faces liability for its disclosures and customer notification practices following the December 2013 data breach.<sup>18</sup> After the true magnitude of the breach was finally revealed, defendants Jacob and Steinhafel "resigned" from their respective positions as Chief Information Officer ("CIO") and Chief Executive Officer ("CEO"). ¶¶15, 16, 122, 124. Despite defendant Steinhafel's acknowledgment of responsibility for the breach, the Board permitted defendant Steinhafel to retain lucrative compensation and severance benefits. ¶¶15, 121, 131(g). In evaluating whether the Individual Defendants' response to the data breach was consistent with their fiduciary duties to the Company, the SLC should also consider the circumstances surrounding the "resignation" of defendants Jacob and Steinhafel.

At a minimum, the SLC should ask the following questions during witness interviews:

---

<sup>18</sup> Forty-six states, plus the District of Columbia, have passed data privacy laws requiring entities sustaining a data breach to promptly notify any individual whose personal information was, or was reasonably believed to have been, compromised.

- What policies and procedures were in place governing Target's response to a data breach and what were the consequences for any failure to follow them? Were they followed after the December 2013 data breach? Did any of the Individual Defendants review or approve any of these policies or procedures?
- How did each of the Individual Defendants respond upon learning of the December 2013 data breach?
- Who was responsible for determining what Target would disclose regarding the data breach?
- Did the Board discuss any of the Company's disclosures regarding the data breach? Who advised the Board regarding the Company's disclosures?
- Did the Board evaluate or approve any public statements regarding the data breach made by individuals at the Company, including defendant Steinhafel?
- What remedial measures were taken at Target following the December 2013 data breach, including, without limitation, any changes to personnel, policies, or technologies?
- Does the Board currently believe that it is receiving adequate information about vulnerabilities or risks posed by the Company's information security systems and that the Company's cybersecurity risk management practices are sufficient?

### **C. Witnesses to Interview**

In order to adequately evaluate the Individual Defendants' liability and identify additional individuals that are responsible for causing damages to Target, the SLC should interview all of the Individual Defendants and the following current and former Target employees:

1. SOC manager, Brian Bobo (*former*)
2. Security Expert, Brian Krebs
3. CISO, Brad Maiorino
4. Target spokeswoman, Molly Snyder
5. Chief Compliance Officer, Ann Scovil
6. VP of Infrastructure and Security, Jeff Mader
7. VP of Information Security and Risk, Adrian Butler

8. VP, IT Support and Operations, Anne Murphy
9. Senior Director of Information Protection, Brenda Bjerke
10. Senior Group Manager of Information Security, Jeremy Milburn
11. Senior Group Manager of Information Protection, Melissa Seebeck
12. Senior Group Manager of Information Protection, Jadee Hanson
13. Manager of Risk Assessment Team, Timothy Rounds
14. Manager of Information Protection, Cody Chamberlain
15. Manager of Information Protection, Todd Thorsen
16. Manager of Information Protection, Tony James
17. General Manager of IT Security and Compliance, Mike Lexa
18. Manager of IT Security Governance & Controls, Milinda Rambel
19. Manager of Cyber Intelligence, Ryan Aniol
20. Manager, Compliance Risk Assessment, Amy Ruge
21. Manager, Cyber and Global Intelligence, Karl Mattson (*former*)

The SLC should also consider whether to interview other Target employees and employees of FireEye and Symantec who developed, installed, or monitored the cyber security products or platforms provided by FireEye or Symantec, including any alerts. Further, the SLC should evaluate whether to interview the following Target employees:

1. SVP, Technology Strategy & Business Solutions, Tom Butterfield
2. Senior Director, Enterprise Architecture, Kim Skanson
3. Director, Enterprise Architecture, Keith Tanski
4. Director, IT Operations, Nick Underwood
5. Director, Target Technology Services, Karl Baltes
6. Senior Group Manager, Global Crisis Management & Business Continuity, Bryan Strawser

Finally, the SLC should review all documents and interview all document custodians identified by defense counsel in connection with discovery in the pending litigation involving the Company.

#### IV. REMEDIAL MEASURES

While Target has implemented some remedial measures in the wake of the breach, hackers are intelligent and opportunistic and will continue to actively search for and exploit weaknesses and vulnerabilities in the Company's information security systems. The Board has a duty to Target shareholders and customers to be vigilant about managing cybersecurity risks and to devote adequate resources to effectively detect, deter, and minimize future breaches of the Company's information security systems. The SLC should evaluate Target's corporate governance and recommend that the Board adopt and implement additional reforms that will help to prevent recurrence of similar harm at Target.

##### A. Third-Party Advisors

The SLC should engage a third-party consulting firm and/or expert in the field of cyber risk management to assist in its evaluation of Target's corporate governance, such as one of the following qualified candidates:

- **Global Cyber Risk LLC** (Jody Westby, Esq., CEO)<sup>19</sup>
  - Specializes in offering assistance to boards and senior executives in managing cyber risks and exercising effective oversight; development and maintenance of enterprise security programs.
- **The Anfield Group**<sup>20</sup>
  - Specializes in governance and risk consulting
- **James Andrew Lewis**, Director and Senior Fellow, Strategic Technologies Program, Center for Strategic and International Studies<sup>21</sup>

---

<sup>19</sup> <http://globalcyberrisk.com/>

<sup>20</sup> <http://theanfieldgroup.com/>

<sup>21</sup> <https://csis.org/expert/james-andrew-lewis>

- Specialties include cybersecurity and governance

## **B. Corporate Governance Reforms**

The SLC should also recommend that Target adopt the following corporate governance reforms:

### **1. Risk Management Committee**

Target's Audit Committee failed to put in place the people, procedures and technology to prevent one of the largest data breaches in corporate history. The Board charged the Audit Committee with reviewing management's approach to risk management, but it left "primary responsibility" for risk management with Company management. ¶62.<sup>22</sup> This contributed to the problems surrounding the data breach. Given the Audit Committee's significant responsibilities with respect to the Company's financial statements, the Audit Committee's ability to effectively oversee the Company's risk management function is limited. Target must improve its management of risk, particularly through enhanced Board oversight of the Company's cybersecurity risk management.

The SLC should recommend that Target create a Risk Management Committee. Many commenters have recognized that establishing a Risk Management Committee with primary responsibility for enterprise risks, including cybersecurity risks, is one of the best ways to ensure proper management and oversight of data breach threats.<sup>23</sup> The Board's oversight of Target's

---

<sup>22</sup> Target does not have any Board-level committee that is dedicated solely to oversight of risk management or that is charged with responsibility for overseeing information security. ¶62. *See also* ¶125 (discussing ISS's recommendation that Target's Audit Committee members be removed from the Board due to their failure to adequately manage data security risks).

<sup>23</sup> *See, e.g.,* Governance of Enterprise Security: CyLab 2012 Report May 16, 2012 by Jody Westby P.26 (The "Westby Report"); *see also* Gallardo, Eduardo and Kaplan, Andrew "Board of Directors Duty of Oversight and Cybersecurity" *Delaware Business Court Insider*, August 20, 2014 *available at* [www.gibsondunn.com/publications/Documents/GallardoKaplan--Board-of-Directors-Duty-of-Oversight-Aud2014.pdf](http://www.gibsondunn.com/publications/Documents/GallardoKaplan--Board-of-Directors-Duty-of-Oversight-Aud2014.pdf) (acknowledging the amended complaint and recommending that the enterprise risk committee assume responsibility to ensure oversight and understanding of cybersecurity controls, among other things).



information security would be significantly enhanced by the creation of a separate Risk Management Committee dedicated solely to overseeing the Company's risk management function and specifically charged with oversight of cybersecurity risk management. Suggestions for the role, composition, responsibilities, and duties of the Risk Management Committee include the following:

**a. Purpose and Role of the Risk Management Committee.** The Risk Management Committee shall be charged with assisting the Board in overseeing Target's internal audit function and risk management practices, to the extent that they relate to non-financial legal and regulatory compliance and risk management. The Risk Management Committee shall be responsible for reviewing and approving the Company's cybersecurity risk management practices, policies, and procedures, and Target's Chief Information Security Officer ("CISO") and CIO shall report directly to the Risk Management Committee.<sup>24</sup>

**b. Membership of the Risk Management Committee.** The Risk Management Committee shall be comprised of at least three (3) independent directors who have experience in risk mitigation and/or information security. The Board should consider appointing one or more new independent directors with a background in cybersecurity risk management to serve on the Risk Management Committee. At least one member of the Risk Management Committee shall serve concurrently on the Audit Committee.

**c. Specific Responsibilities of the Risk Management Committee.** Together with the CISO and CIO, the Risk Management Committee should conduct a full-scale review of the policies and procedures that govern cybersecurity risk management and ensure that Target's information security practices comply with current best practices.<sup>25</sup> The Risk Management Committee should also be responsible for:

- (i) Developing and overseeing the implementation of policies and procedures designed to ensure that the Target Information Protection Team receives and adequately responds to warnings regarding potential cybersecurity attacks, including reporting procedures that enable the Risk Management Committee to learn of material risks to Target's information security systems in real-time and oversee the Company's response to such risks.
- (ii) Reviewing and approving the roles and lines of reporting for employees with responsibility for IT risk management. The CISO and CIO shall

<sup>24</sup> Since the data breach, Target has established the position of CISO and hired a new CIO.

<sup>25</sup> See ¶¶69-108.

ensure that reporting structures relating to privacy and security issues remain separate and that the responsibilities of each group are appropriately assigned.<sup>26</sup>

- (iii) Developing and overseeing the implementation of policies and procedures to identify and manage material risks to Target's information security systems, and ensuring the adequacy of the resources Target allocates to its information security systems and cybersecurity risk management procedures.
- (iv) Developing and overseeing the implementation of policies and procedures designed to mitigate cybersecurity risks arising from companies' relationships with third-parties, such as vendors and contractors.<sup>27</sup>
- (v) Reviewing developments and emerging trends relating that affect or could affect the Company's compliance with applicable regulations or laws relating to information security and cybersecurity risk management, including reviewing and approving the Company's disclosures regarding material risks to Target's information security systems, in consultation with the Audit Committee.

**d. Reporting Duties.** The Risk Management Committee should keep the Board apprised of its activities and shall directly advise the Board of its material findings on a periodic basis. The Risk Management Committee shall annually prepare a written report to the Board summarizing its activities, conclusions, and recommendations for the past year and its agenda for the coming year. The Risk Management Committee will regularly report directly to the entire Board all significant findings concerning material risks to Target's information security systems in sufficient detail to allow the Board to exercise meaningful oversight of the Company's information security and cybersecurity risk management practices.<sup>28</sup>

**e. Third-Party Advisors.** Because preventing future data security breaches of similar magnitude will require constant vigilance and proactive deterrence, the Risk Management Committee should periodically engage third-party consulting firm or expert(s) in the field of information security to assist it with risk assessments, risk

---

<sup>26</sup> See Westby Report p.26.

<sup>27</sup> In recent speeches, U.S. Comptroller of the Currency Thomas J. Curry has expressed concerns about cybersecurity risks arising from companies' relationships with third-parties, such as vendors and contractors. Thomas J. Curry, U.S. Comptroller of the Currency, Remarks before the CES Government (Apr. 14, 2014); Remarks before the New England Council (May 16, 2014).

<sup>28</sup> When TJX's board charged its audit committee with overseeing the security of the Company's computer system with respect to customer data, it also required the committee to report to the entire board regarding the security of the company's computer system at least once per year.

management and compliance with the NIST Framework (described further below at Section 2), such as one of the third parties listed above at Section IV.A.<sup>29</sup>

f. **Scope of Authority.** The Risk Management Committee shall have authority and appropriate funds to retain, consult with, and compensate outside counsel and other advisors as the Committee may deem appropriate.

## 2. National Institute of Standards and Technology Framework

The National Institute of Standards and Technology published Version 1.0 of the Framework for Improving Critical Infrastructure Cybersecurity (the "NIST Framework") on February 12, 2014 in response to an Executive Order. The NIST Framework "focuses on using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the organization's risk management processes[.]" referencing globally recognized standards for cybersecurity.<sup>30</sup> The Securities and Exchange Commission's ("SEC") Office of Compliance Inspections and Examinations recently stated that it would look to the NIST Framework when conducting examinations of public companies regarding cyber security measures.<sup>31</sup> Corporate counsel around the country also have discussed the importance of implementing the NIST Framework to protect companies against cyber-attacks, suggesting that a board that fails to implement this framework may fail to adequately fulfill its fiduciary duty of due care.<sup>32</sup>

The SLC should recommend that Target's Board, via the Risk Management Committee, oversee management's implementation of the NIST Framework at the Company.

---

<sup>29</sup> According to Westby, many boards of directors rely solely on the IT risk expertise of their insurance brokers. *See* Westby Report 19-20. Engaging an expert dedicated to improving corporate risk management, however, is a far better practice for companies that are common targets of cyber attacks. JPMorgan, for example, routinely engages third-party service providers as part of the company's continual efforts to enhance the company's defense against cyber attacks and improve its resiliency to cybersecurity threats.

<sup>30</sup> NIST Framework, Executive Summary, *available at* 1.

<sup>31</sup> *See* SEC National Exam Program Risk Alert, April 15, 2014.

<sup>32</sup> *See, e.g.,* "Guest Post: Cybersecurity and Cyber Governance: Understanding and Implementing the NIST Cybersecurity Framework" by Tom Conkle and Paul Ferillo, Aug. 13, 2014, *available at* [www.dandodiary.com](http://www.dandodiary.com)

### 3. Chief Compliance Officer

The SLC should recommend that Target hire a new Chief Compliance Officer ("CCO") immediately. The Company has publicly discussed hiring a CCO but has not yet done so. Target's CCO should have executive-level experience in risk mitigation and enterprise security and/or must hire a direct subordinate officer with at least three years' experience in these areas.

The responsibilities and duties of the Company's CCO shall include the following:

a. Working with the Audit Committee to evaluate and define the goals of the Company's ethics and compliance programs, in which capacity the CCO shall: (1) implement a program of measurement to monitor performance of the Company's ethics and compliance programs; (2) periodically report to the Audit Committee regarding the performance of the Company's ethics and compliance programs and progress toward program goals; and (3) make written recommendations regarding modifications to the Company's ethics and compliance programs on at least an annual basis.

b. Serving on the Company's information security risk management team and acting as the liaison between the team and the Audit Committee, in which capacity the CCO shall: (1) be primarily responsible for assessing organizational risk relating to misconduct and noncompliance with applicable laws, regulations, and cybersecurity risk management best practices; (2) report material risks relating to compliance issues to the Audit Committee; and (3) make written recommendations for further evaluation and/or remedial action.

### 4. Information Security Risk Management Team

Target should establish a management-level, enterprise-wide information security risk management team (the "ISRM Team") comprised of C-level employees including the CEO, CCO, CIO, and CISO.<sup>33</sup> The ISRM Team should develop policies and procedures that are consistent with the NIST Framework and report to the Board at least quarterly regarding Target's compliance with the NIST Framework, including any subsequent versions of the framework.

The ISRM Team should also have primary responsibility for reporting to the Board any material risks relating to the Company's information security systems. The ISRM Team should be charged with overseeing internal audits of Target's the Company's internal controls and procedures relating to privacy compliance, incident response, breach notification, disaster

---

<sup>33</sup> See Westby Report at \_\_\_ (suggesting establishment of cross-organizational management-level enterprise risk management team).

recovery, and crisis communication plans. Following completion of these audits, the ISRM Team should report all significant changes to these internal controls that have resulted or may result in material changes to the Company's risk profile to the Audit and Risk Management Committees.

#### **5. Disclosures Relating to Cybersecurity Risks and Cyber Incidents**

In 2011, the SEC issued guidance regarding disclosure obligations relating to cybersecurity risks and cyber incidents.<sup>34</sup> SEC Chairwoman Mary Jo White has emphasized that the SEC's guidance makes clear that "material information regarding cybersecurity risks and cyber incidents is *required* to be disclosed."<sup>35</sup> Target's Form 10-Q filed November 27, 2013 – the same day the data breach began – failed to disclose *any* information regarding cybersecurity risks, confirming that Target's Board has failed to prioritize the Company's compliance with the SEC's guidance.

The SLC should recommend that Target's Board require that Company disclosures comply with the SEC's Division of Corporate Finance Disclosure Guidance: Topic No. 2 (Cybersecurity).<sup>36</sup> Target's Audit Committee, in consultation with the Risk Management Committee, should oversee the implementation of procedures that will enable it to effectively evaluate the sufficiency of the Company's disclosures in light of the SEC's guidance.

#### **6. Improve Director Education and Training**

SEC Commissioner Luis Aguilar recently noted that many boards lack the technical expertise necessary to be able to evaluate whether management is taking appropriate steps to

---

<sup>34</sup> Division of Corporate Finance, SEC, CF Disclosure Guidance: Topic No. 2 (Cybersecurity), dated October 13, 2011, *available at* <http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm>.

<sup>35</sup> Opening Remarks, SEC roundtable on cybersecurity, March 26, 2014 (emphasis added).

<sup>36</sup> Leading federal courts have considered SEC guidance in evaluating the sufficiency of companies' public disclosures. *See, e.g., In re Fuwei Films Sec. Litig.*, 634 F. Supp. 2d 419, 443 (S.D.N.Y. 2009).

address cyber security issues.<sup>37</sup> Further, Aguilar acknowledged that various academics have suggested imposing requirements of Board-level or Risk/Audit Committee expertise in cyber security may be necessary for a board to adequately fulfill its fiduciary duties.

The SLC should recommend that Target require each member of the Board to attend annually at least one continuing education program regarding information security and/or cybersecurity risk management best practices. In addition, Target's CIO and CISO, in consultation with the Risk Management Committee and Audit Committee, should formulate written materials to be disseminated to all Target directors on an annual basis that outline and discuss developments and emerging trends relating to information security and cybersecurity risk management best practices.

## **7. Cybersecurity Insurance**

Target maintains \$100 million of network security-insurance coverage, above a \$10 million deductible and with a \$50 million sublimit for settlements with the payment card networks.<sup>38</sup> The Company also maintains other customary business-insurance coverage that may cover some expenses related to the data breach.<sup>39</sup> Because most general commercial liability policies only cover losses to tangible property, many businesses have been denied insurance coverage for damages and legal defense costs arising from a data breach.<sup>40</sup>

The SLC should recommend that the Board (particularly the Audit Committee and/or Risk Management Committee members) review Target's existing insurance policies and

---

<sup>37</sup> "Boards of Directors, Corporate Governance and Cyber-Risks: Sharpening the Focus" by Luis Aguilar, June 10, 2014 New York NY, *available at* <http://www.sec.gov>.

<sup>38</sup> Target Form 10-Q, filed August 27, 2014.

<sup>39</sup> *Id.*

<sup>40</sup> *See, e.g., Zurich Am. Ins. Co. v. Sony Corp. of Am.*, No. 651982 (Sup. Ct. N.Y. Cnty.) (appeal pending).

determine whether additional insurance coverage would be cost-effective.<sup>41</sup>

## V. CONCLUSION

Upon the completion of its investigation, the SLC should disclose its findings and conclusions to Plaintiffs. The Board should also consider publicly disclosing the SLC's findings, as such transparency could go a long way toward mitigating the reputational damage Target has sustained as a result of the December 2013 data breach.

---

<sup>41</sup> See "Cybersecurity: Breaching the Boardroom" by Ariel Yehezkel and Thomas Michael, March 17, 2014.

GASKINS  
BENNETT  
BIRRELL  
SCHUPP

STEVE GASKINS  
(612) 333-9503  
sgaskins@gaskinsbennett.com

December 3, 2015

Shane P. Sanders, Esq.  
Robbins Arroyo LLP  
600 B St., Suite 1900  
San Diego, CA 92101

Andrew S. Friedman, Esq.  
Bonnett, Fairbourn, Friedman & Balint, P.C.  
2325 E. Camelback Rd., Suite 300  
Phoenix, AZ 85012

Myles A. Schneider, Esq.  
Myles A. Schneider & Assoc., Ltd.  
710 Dodge Avenue NW, Suite A  
Elk River, MN 55330

**Re: *Davis, et al. v. Steinhafel, et al. v. Target Corporation*, Lead Case No. 14-cv-00203  
*Koenke, et al. v. Austin, et al. v. Target Corporation*, Case No. 27-cv-14-1832  
Special Litigation Committee of the Board of Directors of Target Corporation**

Dear Counsel:

As you know, we represent the Special Litigation Committee of Target Corporation's Board of Directors. The SLC is investigating the allegations set forth in a demand and those set forth in the derivative complaints you filed against certain of Target's current and former officers and directors. The allegations generally arise out of a data breach that occurred in November and December of 2013. The derivative actions have been stayed pending the SLC's investigation, and the SLC has provided counsel for the interested parties with regular letters advising them of its activities.

So because of those letters you are aware that in conducting its investigation to date, the SLC has met numerous times, conducted numerous interviews, and requested and reviewed numerous documents and that it has substantially completed the investigative phase of its work. Earlier, at the outset of its investigation, the SLC invited you to share with it your information about and your perspective on the allegations of the derivative complaints. You accepted and provided your perspective in a letter and in a telephone conference. And now that the SLC has arrived at the deliberative phase of its investigation, it would like to give you the opportunity to submit any additional information or argument you believe it should consider in determining whether Target possesses rights and remedies against the parties named in your complaint and, if so, whether it is in the company's best interests to pursue them.

Please let us know if you would like to avail yourselves of this additional opportunity to present your views to the SLC, and, if so, we will schedule your presentation at a mutually convenient time.



GASKINS  
BENNETT  
BIRRELL  
SCHUPP

December 3, 2015  
Page 2

If you have any questions or comments, or wish to set up a presentation, please feel free to call me or attorney Sara Daggett, who is fully familiar with this matter, at 612-333-9500.

Sincerely yours,

A handwritten signature in black ink, appearing to read "Steve Gaskins", with a stylized flourish at the end.

Steve Gaskins

SWG/jt

## Sara H. Daggett

---

**From:** Steve W. Gaskins  
**Sent:** Monday, January 25, 2016 4:49 PM  
**To:** Shane P. Sanders  
**Cc:** 'Justice Kathleen Blatz (kathleenblatz@msn.com) (kathleenblatz@msn.com)'; John Matheson (mathe001@umn.edu); Sara H. Daggett; Dan P. Brees  
**Subject:** Target SLC

Dear Shane,

On December 3 we wrote to you, Andy Friedman, and Myles Schneider to provide the derivative plaintiff shareholders an opportunity to submit any additional information or argument you believe the SLC should consider in its deliberations. Thereafter, on December 22, we had a conference call with you to discuss whether you intended make a presentation. You indicated that you would get back to us on that and on whether the state-court plaintiffs would be included.

This will confirm that we spoke today, and that you do intend to have a further conversation with the SLC, most likely by phone conference, and that you will get back to me with dates for the very near future. You also noted that would be attempting to coordinate with the derivative shareholder plaintiffs in the state court action as well, specifically with Andy Friedman.

I look forward to hearing back from you about dates tomorrow. If you have any questions or comments, please feel free to call me.

Sincerely yours,

Steve W. Gaskins  
Gaskins Bennett Birrell Schupp LLP  
333 South 7th Street, Suite 3000, Minneapolis, MN 55402-2440  
[www.gaskinsbennett.com](http://www.gaskinsbennett.com)  
[sgaskins@gaskinsbennett.com](mailto:sgaskins@gaskinsbennett.com)  
TEL 612-333-9503 / FAX 612-333-9579

[My Bio](#)  
[My V-Card](#)  
[Map/Directions](#)

---

**CONFIDENTIALITY NOTICE:** This message contains confidential information intended for use of the named addressee(s) and may contain proprietary and/or legally privileged information. If you are not the designated recipient, you may not read, copy, distribute or retain this message. If you received this message in error, please notify the sender at (612) 333-9500, and destroy and delete it from your system. This message and any attachments are covered by the Electronic Communications Privacy Act, 18 U.S.C. §§ 2510-2521.

GASKINS  
BENNETT  
BIRRELL  
SCHUPP

STEVE GASKINS  
(612) 333-9503  
sgaskins@gaskinsbennett.com

February 5, 2016

Shane P. Sanders, Esq.  
Robbins Arroyo LLP  
600 B St., Suite 1900  
San Diego, CA 92101

**Re: *Davis, et al. v. Steinhafel, et al. v. Target Corporation*, Lead Case No. 14-cv-00203  
*Koenke, et al. v. Austin, et al. v. Target Corporation*, Case No. 27-cv-14-1832  
Special Litigation Committee of the Board of Directors of Target Corporation**

Dear Shane:

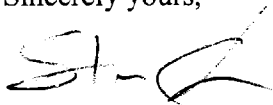
Thank you for your letter of January 28. The SLC has reviewed it and will take it into consideration as it prepares its report.

You have requested the SLC to share with you information from its investigation before you make a supplemental presentation. As to that, please understand that the SLC will not share the information it has gathered or its conclusions with anyone before it issues its report. The reason for this is that it is vital for the SLC to maintain its independence.

Nevertheless it is important that the SLC receive any information, whether from a document or witness, that you believe supports a finding of liability under the applicable law against any of the named defendants. That is why the SLC has invited you to supplement the presentation you made in the early stages of the investigation. So we trust that if you have something important, you will share it.

If you do have significant information to share with the SLC, please let us know promptly. Absent a substantial reason for delay, the SLC needs to hear from you by February 18, 2016.

Sincerely yours,



Steve Gaskins

SWG/jt



600 B Street, Suite 1900  
San Diego, CA 92101  
619.525.3990 phone  
619.525.3991 fax  
www.robbsinarroyo.com

February 19, 2016

**VIA E-MAIL AND U.S. MAIL**

sgaskins@gaskinsbennett.com

Steve Gaskins, Esq.  
GASKINS BENNETT BIRRELL SCHUPP LLP  
333 South Seventh Street, Suite 3000  
Minneapolis, MN 55402

**Re: *In re: Target Corporation Customer Data Security Breach Litigation:  
Shareholder Derivative Action, Lead Case No. 0:14-cv-00203-PAM-JJK  
Special Litigation Committee of the Board of Directors of Target  
Corporation***

Dear Mr. Gaskins:

We are in receipt of your February 5, 2016 letter. We are disappointed in the SLC's blanket refusal to provide Plaintiffs *any* information whatsoever about the actions it has taken as proposed in Plaintiffs' October 2, 2014 letter to the SLC, or to identify which documents referenced therein have been reviewed and which witnesses identified therein have been interviewed. The SLC's decision to keep Plaintiffs in the dark has precluded more meaningful and valuable interactions between Plaintiffs and the SLC. Nonetheless, in the interest of continuing to serve the best interests of the Company, Plaintiffs have prepared a written submission to the SLC, which is attached hereto as Schedule A. Our submission outlines: (i) certain post-filing information we uncovered during our investigation of the cyber-attack; and (ii) the legal standards applicable to breaches of fiduciary duty under Minnesota corporate law as it relates to exculpatory provisions in corporations' articles of incorporation. The additional information discovered in connection with Plaintiffs' investigation shall be used only in connection with the SLC's investigation and any related discussions between Plaintiffs and the SLC, and otherwise shall be kept confidential. We are available to discuss our findings and/or the relevant legal standards with the SLC, and we remain willing to work with and are still interested in assisting the SLC, including in the potential prosecution of claims on behalf of Target.

Sincerely,

A handwritten signature in black ink, appearing to read 'Shane P. Sanders', is written over a horizontal line.

Shane P. Sanders

**SCHEDULE A****ADDITIONAL INFORMATION REGARDING THE TARGET CYBER-ATTACK**

Plaintiffs have obtained certain additional information regarding the winter 2013 cyber-attack of Target Corporation's ("Target" or the "Company") computer network. Plaintiffs interviewed various sources, including former employees of Target and reporters who covered the cyber-attack in order to determine whether directors and officers of Target had breached their fiduciary duties to the Company. Plaintiffs do not intend to share the names of the sources that provided this information. Some of the sources spoke to Plaintiffs under the condition that their names would not be shared, and the sources provided information about certain reports that shed light on the cyber-attack.

**I. The "Risk Accept" Report**

An executive-level group within Target called the Risk Review Committee ("RRC") met as often as once a month regarding risk management issues affecting Target's business. The RRC spanned a number of teams within Target, including the Information Technology, Security, Risk, and Target Technical Services ("TTS") departments. Two Target employees, Garrett Markin and Erin Getty, worked full-time for the RRC. Various high-level Target employees working in the information technology ("IT") sphere attended RRC meetings: a source mentioned both former Chief Information Officer Beth M. Jacob and the head of TTS, but could not confirm with 100% certainty that both attended.

The RRC studied Target's IT security systems in late 2013 as Target was preparing for the opening of its Canadian stores. For the Canadian stores, Target purchased a new point of sale ("POS") system produced by Retalix.<sup>1</sup> The U.S. stores had utilized a home-grown POS system called the "Domain Center of Excellence" that was known to be less reliable. ¶74.<sup>2</sup> The

---

<sup>1</sup> See [www.retalix.com](http://www.retalix.com). Retalix is a subsidiary of NCR Corporation (NYSE: NCR).

<sup>2</sup> All paragraph references ("¶" or "¶¶") are to Plaintiffs' Verified Consolidated Shareholder Derivative Complaint for Breach of Fiduciary Duty and Waste of Corporate Assets (the "Complaint") filed July 18, 2014 (Dkt. No. 48).

RRC analyzed whether the risk of keeping the U.S. stores on the home-grown POS system justified the cost savings.

The RRC produced a report that has been called the "Risk Accept Report." This report recognized that keeping the home-grown POS system for Target's U.S. stores created substantial risks to Target's IT security, but that this risk was a tolerable one. The Risk Accept Report premised its conclusion on a plan to roll out a new POS system for the U.S. stores over the next five years. It is likely that the Risk Accept Report sheds light on Target employees' knowledge of Target's IT security deficiencies in the time period leading up to the cyber-attack.

One of Plaintiffs' sources, a reporter, spoke with two individuals who had firsthand knowledge of the Risk Accept Report. This source did not publicly print information about the report because some details could not be confirmed with sufficient certainty.

## **II. The Payment Card Industry ("PCI") Forensic Investigation Report (the "PCI Report")**

It is well known that the PCI Security Standards Council ("PCI-SSC") promulgates industry-wide data security standards ("DSS") in order to encourage and enhance cardholder data security.<sup>3</sup> Some states have adopted laws that require compliance with the DSS.<sup>4</sup> The PCI-SSC will regularly assess compliance with its standards, but after a major breach, the PCI-SSC will often conduct a forensic investigation to determine whether a company was retroactively compliant with the DSS, even if it was previously certified as compliant.

The PCI Report contains a retroactive review of Target's data security practices at the time of the cyber-attack. Verizon Enterprise Solutions authored the PCI Report, and the PCI auditor came from a data security company called Trustwave Holdings, Inc. Plaintiffs' source was informed that the PCI Report is damning, but the source had not personally reviewed it. The

---

<sup>3</sup> See, e.g., [www.pcisecuritystandards.org](http://www.pcisecuritystandards.org).

<sup>4</sup> See, e.g., Nev. Rev. Stat. 603A.215; see also James T. Graves, *Minnesota's PCI Law: A Small Step on the Path to a Statutory Duty of Data Security Due Care*, 34 WM. MITCHELL L. REV. 1115, 1116-17 (2008) (recognizing that Minnesota's data security law, Minn. Stat. §325E.64, is based on the DSS).

source was told that the PCI Report details the areas where Target failed in its IT security and risk management practices, and that it speaks to issues relevant to Defendants' breaches of fiduciary duties.<sup>5</sup>

### **III. The Issa Investigation**

Congressman Darrell Issa, former Chairman of the Committee on Oversight and Government Reform of the U.S. House of Representatives, investigated the Target cyber-attack. As part of his investigation, Congressman Issa obtained various internal Target documents that uncover the actions and beliefs of Target employees as they realized that Target had suffered a massive cyber-attack. The documents Issa obtained include e-mail threads and investigative reports and the names of the Target employees who handled these data security issues. According to a source, Target employees felt that IT security had been "put on the backburner" and were not surprised to learn Target had been attacked.

#### **TARGET'S EXCULPATORY PROVISION DOES NOT APPLY TO BREACH OF FIDUCIARY DUTY CLAIMS IN THIS MATTER**

In Minnesota, a director's personal liability for a breach of fiduciary duty may be limited by a corporation's articles of incorporation. Minn. Stat. §302A.251(4). Specifically, Subdivision 4 states that a "director's personal liability to the corporation or its shareholders for monetary damages for breach of fiduciary duty as a director may be eliminated or limited in the articles," but that the articles "shall not eliminate or limit the liability of a director: (a) for any breach of the director's duty of loyalty to the corporation or its shareholders; [or] (b) for acts or omissions not in good faith or that involve intentional misconduct or a knowing violation of law." Delaware law, to which Minnesota courts look for guidance,<sup>6</sup> contains a similar statute and

---

<sup>5</sup> "Defendants" refers to Gregg W. Steinhafel, Beth M. Jacob, James A. Johnson, John Mulligan, Anne M. Mulcahy, Roxanne S. Austin, Calvin Darden, Mary E. Minnick, Derica W. Rice, John G. Stumpf, Douglas M. Baker, Jr., Henrique De Castro, Kenneth L. Salazar, Solomon D. Trujillo, and nominal defendant Target.

<sup>6</sup> Because shareholder derivative actions in Minnesota are rare, Minnesota courts often look to the decisions of Delaware courts. *See In re Xcel Energy, Inc.*, 222 F.R.D. 603, 606 (D. Minn.

virtually identical limitations on a corporation's ability to limit the personal liability of its directors for monetary damages. *See* 8 Del. C. §102(b)(7) (directors cannot seek protection for "any breach of the director's duty of loyalty" or "acts or omissions not in good faith"); *In re Zoran Corp. Derivative Litig.*, 511 F. Supp. 2d 986, 1017 (2007) (a breach of the duty of loyalty is an un-exculpable claim); *Ryan v. Lyondell Chem. Co.*, C.A. No. 3176-VCN, 2008 WL 4174038, at \*3 (Del. Ch. Aug. 29, 2008) ("a conscious disregard of one's responsibilities" is "properly treated as a non-exculpable, non-indemnifiable violation of the fiduciary duty to act in good faith"), *rev'd on other grounds*, 970 A.2d 235 (Del. 2009).

Here, it appears that Target's Articles of Incorporation contain an exculpatory clause providing that the Company's directors will not be liable for breaches of fiduciary duty unless they breach the duty of loyalty, act in bad faith, engage in intentional misconduct, or commit a knowing violation of law. Target's exculpatory provision is, thus, limited—it only: (i) exculpates directors for acts taken in their capacity as directors, not as officers or employees of the Company; and (ii) applies to breaches of the duty of care, and expressly does not apply to any breach of the director's duty of loyalty and acts or omissions not in good faith or which involve intentional misconduct or a knowing violation of the law. *See* Article IV, Amended and Restated Articles of Incorporation of Target Corporation (as amended through June 9, 2010).

"The duty of loyalty ... is violated '[w]here directors fail to act in the face of a known duty to act, thereby demonstrating a conscious disregard for their responsibilities [and] failing to discharge [the non-exculpable fiduciary duty of loyalty] in good faith.'" *Rosenbloom v. Pyott*, 765 F.3d 1137, 1150 (9th Cir. 2014) (quoting *Stone ex rel. AmSouth Bancorporation v. Ritter*, 911 A.2d 362, 370 (Del. 2006)). Here, Plaintiffs allege that certain of Target's officers and directors utterly and consciously failed to fulfill their duties to implement and oversee the policies, procedures, and people necessary to protect Target's servers from cyber-attacks. ¶¶2-4, 46-108, 117-29, 149-53. Plaintiffs allege that defendants ignored the prior attacks at Target (and

---

2004). Here, as throughout, all emphasis is added and citations and footnotes are omitted unless otherwise noted.



similar attacks at other companies) and the explicit and ever-increasing warnings of serious data security risks that could cause substantial harm to the Company, and failed to update Target's corporate governance or risk management practices or ensure that Target complied with even the most basic and fundamental industry standards for protecting consumer information. *Id.*<sup>7</sup> And, even after the data breach, plaintiffs allege that Defendants consciously failed to act to ensure that the Company timely notified consumers that its information security system had been breached, putting customers at additional risk and causing further damage to Target. ¶¶5, 109-16. Plaintiffs' claims are, thus, based on breaches of the duty of loyalty and good faith, which are non-exculpable claims. Accordingly, if Plaintiffs' allegations and claims are borne out, section 302A.521 of the Minnesota Business Corporation Act would be inapplicable, and the exculpatory provision in Target's Articles of Incorporation would not prevent or otherwise limit Plaintiffs' and/or the Company's ability to recover from the wrongdoers.

---

<sup>7</sup> By way of example, Target did not follow standard IT security practices, failed to ensure that individuals with the requisite expertise and understanding of data security issues were appointed to appropriate positions and that a Chief Information Security Officer with the ability to explain the risks and vulnerabilities to the Defendants was in place, and published extensive information about its computer system on the Internet. ¶¶2-6, 46-108, 129.

**GASKINS  
BENNETT  
BIRRELL  
SCHUPP**

STEVE GASKINS  
(612) 333-9503  
sgaskins@gaskinsbennett.com

February 24, 2016

Shane P. Sanders, Esq.  
Robbins Arroyo LLP  
600 B St., Suite 1900  
San Diego, CA 92101

**Re: *Davis, et al. v. Steinhafel, et al. v. Target Corporation*, Lead Case No. 14-cv-00203  
*Koenke, et al. v. Austin, et al. v. Target Corporation*, Case No. 27-cv-14-1832  
Special Litigation Committee of the Board of Directors of Target Corporation**

Dear Shane:

Thank you for your letter of February 19. The SLC appreciates the help you have offered and your interest in assisting the investigation. However, it is important to understand that while the SLC can consider others' investigations, it must also conduct its own and do so independently.

The SLC has read and considered your February 19 letter and Schedule A attached to it, as it did your October 2, 2014 letter.

The SLC also appreciates that you are available to discuss with it your findings and your view of the relevant legal standards. The SLC has a scheduled meeting the afternoon of March 1 beginning at 1:30 p.m., CST, and invites you to discuss your findings and your view of the relevant legal standards with it that day. We suggest a half-hour any time between 1:30 and 5:00 p.m., CST (11:30 a.m. – 3:00 p.m., PST) at your convenience next Tuesday, March 1.

Please let me know as soon as possible what time would be best for you.

Sincerely yours,



Steve Gaskins

SWG/jt

**Dan P. Brees**

---

**From:** Steve W. Gaskins  
**Sent:** Tuesday, March 01, 2016 1:04 PM  
**To:** Shane P. Sanders  
**Cc:** Dan P. Brees; Ian S. Birrell  
**Subject:** RE: Target - 3/1/16 SLC Meeting

Dear Shane—

Thanks for the reply. I will discuss it with the Committee this afternoon.

Sincerely yours,

Steve W. Gaskins  
Gaskins Bennett Birrell Schupp LLP  
333 South 7th Street, Suite 3000, Minneapolis, MN 55402-2440  
[www.gaskinsbennett.com](http://www.gaskinsbennett.com)  
[sgaskins@gaskinsbennett.com](mailto:sgaskins@gaskinsbennett.com)  
TEL 612-333-9503 / FAX 612-333-9579

[My Bio](#)  
[My V-Card](#)  
[Map/Directions](#)

---

**CONFIDENTIALITY NOTICE:** This message contains confidential information intended for use of the named addressee(s) and may contain proprietary and/or legally privileged information. If you are not the designated recipient, you may not read, copy, distribute or retain this message. If you received this message in error, please notify the sender at (612) 333-9500, and destroy and delete it from your system. This message and any attachments are covered by the Electronic Communications Privacy Act, 18 U.S.C. §§ 2510-2521.

---

**From:** Shane P. Sanders [<mailto:SSanders@robbinsarroyo.com>]  
**Sent:** Tuesday, March 01, 2016 12:47 PM  
**To:** Steve W. Gaskins  
**Subject:** Target - 3/1/16 SLC Meeting

Hi, Steve. I got your voicemail. I am actually traveling today (and specifically during the window of time outlined in your letter from Thursday), and so I am not able to join the SLC's scheduled meeting this afternoon. As I have indicated, we believe the SLC's decision to not provide any information regarding what has and has not been done in connection with its investigation (particularly with regard to the specific steps we believe are critical and which we outlined in detail back in 2014) ultimately limits our ability to meaningfully participate. That said, if there are specific questions or issues either you or the SLC would like to discuss, I am happy to try to figure out a time that works. Thank you.

Shane P. Sanders  
Attorney at Law  
Robbins Arroyo LLP  
600 B Street, Suite 1900  
San Diego, CA 92101  
Telephone: (619) 525-3990  
Facsimile: (619) 525-3991  
Email: [SSanders@robbinsarroyo.com](mailto:SSanders@robbinsarroyo.com)  
[www.robbinsarroyo.com](http://www.robbinsarroyo.com)

This message and any attached documents contain information from the law firm of Robbins Arroyo LLP that may be privileged, confidential and/or exempt from disclosure under applicable law. If you are not the intended recipient, you may not read, copy, distribute or use this information. If you have received this email in error, please notify the sender and/or Robbins Arroyo LLP immediately by reply email and/or by telephone at (619) 525-3990 and delete this copy from your email system. Thank you.



Please consider the environment before printing this email.

**GASKINS  
BENNETT  
BIRRELL  
SCHUPP**

STEVE GASKINS  
(612) 333-9503  
sgaskins@gaskinsbennett.com

July 24, 2014

Robert B. Weiser, Esq.  
The Weiser Law Firm  
22 Cassatt Ave.  
Berwyn, PA 19312

**Re: Special Litigation Committee of the Board of Directors of Target Corporation  
Our File No. 19767**

Dear Mr. Weiser:

We represent the Special Litigation Committee of Target's Board of Directors, which is investigating the May 2, 2014 shareholder demand of the Paul Perry Revocable Living Trust. The SLC consists of two distinguished jurists, Chief Justice of the Minnesota Supreme Court (ret.) Kathleen Blatz and Professor John Matheson, who, before their appointment to the SLC, were not associated with Target.

The investigation is in its beginning stage and the SLC would very much like to get your input on the issues raised in the demand you made on behalf of Mr. Perry's trust. Accordingly, the SLC has asked us to invite you to make a presentation on the issues arising from the allegations set forth in the demand, including your view of the factors bearing on whether there are rights and remedies Target has against the persons named in your demand that are in Target's best interests to pursue. The following dates and times are presently available:

Wednesday, July 30 at 2:00 pm

Thursday, August 21 at 9:00 am

Thursday, August 28 at 2:00 pm

Please let us know if one of these dates is convenient for you, and we will schedule your presentation. If not, please let us know and we will search for a mutually convenient alternative date.

If you have any questions or comments, or wish to set up a presentation, please feel free to call me or attorney Sara Daggett, who is fully familiar with this matter, at 612-333-9500.

Sincerely yours,



Steve Gaskins  
SWG/jt

**GASKINS  
BENNETT  
BIRRELL  
SCHUPP**

STEVE GASKINS  
(612) 333-9503  
sgaskins@gaskinsbennett.com

December 3, 2015

Robert B. Weiser, Esq.  
The Weiser Law Firm  
22 Cassatt Ave.  
Berwyn, PA 19312

**Re: Special Litigation Committee of the Board of Directors of Target Corporation  
Our File No. 19767**

Dear Mr. Weiser:

As you know, we represent the Special Litigation Committee of Target Corporation's Board of Directors. The SLC is investigating allegations you set forth in the Paul Perry Revocable Living Trust's May 2, 2014 demand to the Board and similar allegations made in certain derivative complaints filed in state and federal courts in Minnesota. Those allegations generally arise out of a data breach that occurred at Target in November and December 2013.

At the outset of the SLC's investigation, we sent you a letter, dated July 24, 2014, inviting you to provide the SLC with your input on the issues raised in the demand you made on behalf of Mr. Perry's trust. But we did not hear back from you, so no meeting or phone conference was scheduled.

Since that time, the SLC has met numerous times, has conducted numerous interviews, and has requested and reviewed numerous documents in its investigation of the issues raised in Mr. Perry's trust's demand and in the derivative complaints. As you no doubt know from the updates of the SLC's activities that have been sent to you, the SLC's investigation has now entered its deliberative phase. And since it has not heard from you, the SLC has asked us to again invite you to provide—by way of an in-person presentation or otherwise—any information or argument on any issues you think relevant to its consideration of whether it is in Target's best interests to pursue claims based on the allegations set forth in the demand you made on behalf of Mr. Perry's trust.

If you are interested in making such a presentation, please let us know and we will work with you to schedule a mutually convenient date.

GASKINS  
BENNETT  
BIRRELL  
SCHUPP

Robert B. Weiser, Esq.  
December 3, 2015  
Page 2

If you have any questions or comments, or wish to set up a presentation, please feel free to call me or attorney Sara Daggett, who is fully familiar with this matter, at 612-333-9500.

Sincerely yours,

A handwritten signature in black ink, appearing to read "Steve Gaskins", with a stylized flourish at the end.

Steve Gaskins

SWG/jt

GASKINS  
BENNETT  
BIRRELL  
SCHUPP

STEVE GASKINS  
(612) 333-9503  
sgaskins@gaskinsbennett.com

December 9, 2015

Robert B. Weiser, Esq.  
The Weiser Law Firm  
22 Cassatt Ave.  
Berwyn, PA 19312

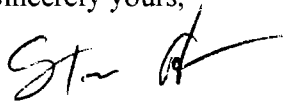
**Re: Special Litigation Committee of the Board of Directors of Target Corporation  
Our File No. 19767**

Dear Mr. Weiser:

On July 24, 2014 and on December 3, 2015, on behalf of the Special Litigation Committee of Target's Board of Directors, we invited you to present any information or argument that you think relevant to the issues before the SLC concerning allegations you made on behalf of the Paul Perry Revocable Living Trust. In both of those letters, we only referred to the demand you made by letter dated May 2, 2014, and did not reference your demand letter dated April 10, 2014. Please be assured that from the outset of the investigation, the Special Litigation Committee has had copies of both demand letters and has been investigating all the issues raised and all the allegations made in them.

If you have any questions or comments, please feel free to call me.

Sincerely yours,



Steve Gaskins

SWG/jt

# **APPENDIX D**



**WRITTEN TESTIMONY**

**BEFORE THE**

**SENATE COMMITTEE ON THE JUDICIARY**

**HEARING ON**

**PRIVACY IN THE DIGITAL AGE:**

**PREVENTING DATA BREACHES AND COMBATING CYBERCRIME**

**FEBRUARY 4, 2014**

**TESTIMONY OF**

**JOHN MULLIGAN**

**EXECUTIVE VICE PRESIDENT AND CHIEF FINANCIAL OFFICER**

**TARGET**

**I. Introduction**

Good morning Chairman Leahy, Ranking Member Grassley, and Members of the Committee. My name is John Mulligan and I am the Executive Vice President and Chief Financial Officer of Target. I appreciate the opportunity to be here today to discuss important issues surrounding data breaches and cybercrime.

As you know, Target recently experienced a data breach resulting from a criminal attack on our systems. To begin, I want to say how deeply sorry we are for the impact this incident has had on our guests – your constituents. We know this breach has shaken their confidence in Target, and we are determined to work very hard to earn it back.

At Target we take our responsibility to our guests very seriously, and this attack has only strengthened our resolve. We will learn from this incident and as a result, we hope to make Target, and our industry, more secure for consumers in the future.

I'd now like to explain the events of the breach as I currently understand them. Please recognize that I may not be able to provide specifics on certain matters because the criminal and forensic investigations remain active and ongoing. We are working closely with the U.S. Secret Service and the U.S. Department of Justice on the investigation – to help them bring to justice the criminals who perpetrated this wide-scale attack on Target, American business and consumers.

## **II. What We Know**

On the evening of December 12, we were notified by the Justice Department of suspicious activity involving payment cards used at Target stores. We immediately started our internal investigation.

On December 13, we met with the Justice Department and the Secret Service. On December 14, we hired an independent team of experts to lead a thorough forensic investigation.

On December 15, we confirmed that criminals had infiltrated our system, had installed malware on our point-of-sale network and had potentially stolen guest payment card data. That same day, we removed the malware from virtually all registers in our U.S. stores.

Over the next two days, we began notifying the payment processors and card networks, preparing to publicly notify our guests and equipping our call centers and stores with the necessary information and resources to address the concerns of our guests.

On December 18 we disabled malware on about 25 additional registers which were disconnected from our system when we completed the initial malware removal on December 15. As a result, we determined that fewer than 150 additional guest accounts were affected.

Our actions leading up to our public announcement on December 19 – and since – have been guided by the principle of serving our guests, and we have been moving as quickly as possible to share accurate and actionable information with the public. When we announced the intrusion on December 19 we used multiple forms of communication, including a mass-scale public announcement, email, prominent notices on our website, and social media channels.

What we know today is that the breach affected two types of data: payment card data which affected approximately 40 million guests and certain personal data which affected up to 70 million guests. The theft of the payment card data affected guests who shopped at our U.S. stores

from November 27 through December 18. The theft of partial personal data included name, mailing address, phone number or email address.

We now know that the intruder stole a vendor's credentials to access our system and place malware on our point-of-sale registers. The malware was designed to capture payment card data from the magnetic strip of credit and debit cards prior to encryption within our system.

As the forensic investigation continued, we learned that the malware also captured some strongly encrypted PIN data. We publicly shared this information on December 27, reassuring our guests that they would not be responsible for any fraudulent charges that may occur as a result of the breach.

When we subsequently confirmed the theft of partial personal data on January 9, we used various channels of communication to notify our guests on January 10 and provide them with tips to guard against possible scams.

### **III. Protecting Our Guests**

From the outset, our response to the breach has been focused on supporting our guests and strengthening our security. In addition to the immediate actions I already described, we are taking the following concrete actions:

- First, we are undertaking an end-to-end review of our entire network and will make security enhancements, as appropriate.
- Second, we increased fraud detection for our Target REDcard guests. To date, we have not seen any fraud on our Target proprietary credit and debit cards due to this breach. And we have seen only a very low amount of additional fraud on our Target Visa card.

- Third, we are reissuing new Target credit or debit cards immediately to any guest who requests one.
- Fourth, we are offering one year of free credit monitoring and identity theft protection to anyone who has ever shopped at our U.S. Target stores. This protection includes a free credit report, daily credit monitoring, identity theft insurance and unlimited access to personalized assistance from a highly trained fraud resolution agent.
- Fifth, we informed our guests that they have zero liability for any fraudulent charges on their cards arising from this incident. We encouraged them to monitor their accounts and promptly alert either Target or their issuing bank of any suspicious activity.
- Sixth, Target is accelerating our investment in chip technology for our Target REDcards and stores' point-of-sale terminals. We believe that chip-enabled technologies are critical to providing enhanced protection for consumers, which is why we are a founding, and steering committee, member of the EMV Migration Forum at the SmartCard Alliance.
- Seventh, Target initiated the creation of, and is investing \$5 million in, a campaign with Better Business Bureau, the National Cyber Security Alliance and the National Cyber-Forensics & Training Alliance to advance public education around cybersecurity and the dangers of consumer scams.
- And, eighth, last week Target helped launch a retail industry Cybersecurity and Data Privacy Initiative that will be focused on informing public dialogue and enhancing practices related to cybersecurity, improved payment security and consumer privacy. Target will be an active leader in this effort.

For many years, Target has invested significant capital and resources in security technology, personnel and processes. We had in place multiple layers of protection, including

firewalls, malware detection software, intrusion detection and prevention capabilities and data loss prevention tools. We perform internal and external validation and benchmarking assessments. And, as recently as September 2013, our systems were certified as compliant with the Payment Card Industry Data Security Standards.

But, the unfortunate reality is that we suffered a breach, and all businesses – and their customers -- are facing increasingly sophisticated threats from cyber criminals. In fact, recent news reports have indicated that several other companies have been subjected to similar attacks.

#### **IV. Moving Forward**

To prevent this from happening again, none of us can go it alone. We need to work together.

Updating payment card technology and strengthening protections for American consumers is a shared responsibility and requires a collective and coordinated response. On behalf of Target, I am committing that we will be an active part of that solution.

Senators -- to each of you, and to all of your constituents and our guests, I want to say once again how sorry we are that this has happened. We will work with you, the business community, and other thought leaders to find effective solutions to this ongoing and pervasive challenge. Thank you very much for your time today.

**WRITTEN TESTIMONY**

**BEFORE THE**  
**HOUSE COMMITTEE ON ENERGY AND COMMERCE**  
**SUBCOMMITTEE ON COMMERCE, MANUFACTURING, AND TRADE**

**HEARING ON**  
**PROTECTING CONSUMER INFORMATION:**  
**CAN DATA BREACHES BE PREVENTED?**

**FEBRUARY 5, 2014**

**TESTIMONY OF**  
**JOHN MULLIGAN**  
**EXECUTIVE VICE PRESIDENT AND CHIEF FINANCIAL OFFICER**  
**TARGET**

**I. Introduction**

Good morning Chairman Terry, Ranking Member Schakowsky, and Members of the Subcommittee. My name is John Mulligan and I am the Executive Vice President and Chief Financial Officer of Target. I appreciate the opportunity to be here today to discuss important issues surrounding data breaches and cybercrime.

As you know, Target recently experienced a data breach resulting from a criminal attack on our systems. To begin, I want to say how deeply sorry we are for the impact this incident has had on our guests – your constituents. We know this breach has shaken their confidence in Target, and we are determined to work very hard to earn it back.

At Target we take our responsibility to our guests very seriously, and this attack has only strengthened our resolve. We will learn from this incident and as a result, we hope to make Target, and our industry, more secure for consumers in the future.

I'd now like to explain the events of the breach as I currently understand them. Please recognize that I may not be able to provide specifics on certain matters because the criminal and forensic investigations remain active and ongoing. We are working closely with the U.S. Secret Service and the U.S. Department of Justice on the investigation – to help them bring to justice the criminals who perpetrated this wide-scale attack on Target, American business and consumers.



## **II. What We Know**

On the evening of December 12, we were notified by the Justice Department of suspicious activity involving payment cards used at Target stores. We immediately started our internal investigation.

On December 13, we met with the Justice Department and the Secret Service. On December 14, we hired an independent team of experts to lead a thorough forensic investigation.

On December 15, we confirmed that criminals had infiltrated our system, had installed malware on our point-of-sale network and had potentially stolen guest payment card data. That same day, we removed the malware from virtually all registers in our U.S. stores.

Over the next two days, we began notifying the payment processors and card networks, preparing to publicly notify our guests and equipping our call centers and stores with the necessary information and resources to address the concerns of our guests.

On December 18 we disabled malware on about 25 additional registers which were disconnected from our system when we completed the initial malware removal on December 15. As a result, we determined that fewer than 150 additional guest accounts were affected.

Our actions leading up to our public announcement on December 19 – and since – have been guided by the principle of serving our guests, and we have been moving as quickly as possible to share accurate and actionable information with the public. When we announced the intrusion on December 19 we used multiple forms of communication, including a mass-scale public announcement, email, prominent notices on our website, and social media channels.

What we know today is that the breach affected two types of data: payment card data which affected approximately 40 million guests and certain personal data which affected up to 70 million guests. The theft of the payment card data affected guests who shopped at our U.S. stores

from November 27 through December 18. The theft of partial personal data included name, mailing address, phone number or email address.

We now know that the intruder stole a vendor's credentials to access our system and place malware on our point-of-sale registers. The malware was designed to capture payment card data from the magnetic strip of credit and debit cards prior to encryption within our system.

As the forensic investigation continued, we learned that the malware also captured some strongly encrypted PIN data. We publicly shared this information on December 27, reassuring our guests that they would not be responsible for any fraudulent charges that may occur as a result of the breach.

When we subsequently confirmed the theft of partial personal data on January 9, we used various channels of communication to notify our guests on January 10 and provide them with tips to guard against possible scams.

### **III. Protecting Our Guests**

From the outset, our response to the breach has been focused on supporting our guests and strengthening our security. In addition to the immediate actions I already described, we are taking the following concrete actions:

- First, we are undertaking an end-to-end review of our entire network and will make security enhancements, as appropriate.
- Second, we increased fraud detection for our Target REDcard guests. To date, we have not seen any fraud on our Target proprietary credit and debit cards due to this breach. And we have seen only a very low amount of additional fraud on our Target Visa card.

- Third, we are reissuing new Target credit or debit cards immediately to any guest who requests one.
- Fourth, we are offering one year of free credit monitoring and identity theft protection to anyone who has ever shopped at our U.S. Target stores. This protection includes a free credit report, daily credit monitoring, identity theft insurance and unlimited access to personalized assistance from a highly trained fraud resolution agent.
- Fifth, we informed our guests that they have zero liability for any fraudulent charges on their cards arising from this incident. We encouraged them to monitor their accounts and promptly alert either Target or their issuing bank of any suspicious activity.
- Sixth, Target is accelerating our investment in chip technology for our Target REDcards and stores' point-of-sale terminals. We believe that chip-enabled technologies are critical to providing enhanced protection for consumers, which is why we are a founding, and steering committee, member of the EMV Migration Forum at the SmartCard Alliance.
- Seventh, Target initiated the creation of, and is investing \$5 million in, a campaign with Better Business Bureau, the National Cyber Security Alliance and the National Cyber-Forensics & Training Alliance to advance public education around cybersecurity and the dangers of consumer scams.
- And, eighth, last week Target helped launch a retail industry Cybersecurity and Data Privacy Initiative that will be focused on informing public dialogue and enhancing practices related to cybersecurity, improved payment security and consumer privacy. Target will be an active leader in this effort.

For many years, Target has invested significant capital and resources in security technology, personnel and processes. We had in place multiple layers of protection, including

firewalls, malware detection software, intrusion detection and prevention capabilities and data loss prevention tools. We perform internal and external validation and benchmarking assessments. And, as recently as September 2013, our systems were certified as compliant with the Payment Card Industry Data Security Standards.

But, the unfortunate reality is that we suffered a breach, and all businesses -- and their customers -- are facing increasingly sophisticated threats from cyber criminals. In fact, recent news reports have indicated that several other companies have been subjected to similar attacks.

#### **IV. Moving Forward**

To prevent this from happening again, none of us can go it alone. We need to work together.

Updating payment card technology and strengthening protections for American consumers is a shared responsibility and requires a collective and coordinated response. On behalf of Target, I am committing that we will be an active part of that solution.

Members of the Subcommittee -- to each of you, and to all of your constituents and our guests, I want to say once again how sorry we are that this has happened. We will work with you, the business community, and other thought leaders to find effective solutions to this ongoing and pervasive challenge. Thank you very much for your time today.

**WRITTEN TESTIMONY**

**BEFORE THE**

**SENATE COMMITTEE ON COMMERCE, SCIENCE, & TRANSPORTATION**

**HEARING ON**

**PROTECTING PERSONAL CONSUMER INFORMATION FROM CYBER ATTACKS**

**AND DATA BREACHES**

**MARCH 26, 2014**

**2:30 PM**

**TESTIMONY OF**

**JOHN MULLIGAN**

**EXECUTIVE VICE PRESIDENT AND CHIEF FINANCIAL OFFICER**

**TARGET**

## **I. Introduction**

Good afternoon Chairman Rockefeller, Ranking Member Thune, and Members of the Committee. My name is John Mulligan and I am the Executive Vice President and Chief Financial Officer of Target. I appreciate the opportunity to be here today to discuss important issues surrounding data breaches and cybercrime.

As you know, Target experienced a data breach in late 2013 resulting from a criminal attack on our systems. Let me reiterate how deeply sorry we are for the impact this incident has had on our guests – your constituents. Our top priority is taking care of our guests. They should feel confident about shopping at Target. We work hard to protect their information. But the reality is we experienced a data breach. Our guests expect more and we are working hard to do better. We know this has shaken their confidence and we intend to earn it back.

We are asking hard questions about whether we could have taken different actions before the breach was discovered that would have resulted in different outcomes. In particular, we are focused on what information we had that could have alerted us to the breach earlier; whether we had the right personnel in the right positions; and ensuring that decisions related to operational and security matters were sound. We are working diligently to answer these questions.

This afternoon, I'd like to provide an update since I last testified, including actions we are taking to further strengthen our security and potential policy solutions we support. Because the government's investigation regarding the intruders remains active and ongoing, I may not be able to provide specifics on certain matters. We continue to work closely with the U.S. Secret Service and the U.S. Department of Justice – to help them bring to justice the criminals who perpetrated this wide-scale attack on Target, American business and consumers.

## **II. What We Know**

We are further strengthening our data security based on learnings from an end-to-end review of our systems. We are not finished with that review, and additional facts may affect our findings, but we are certainly developing a clearer picture of events and want to share with you some key facts we have learned.

Like any large business, we log a significant number of technology activities in our system – more than 1 billion on average each day. These activities range from relatively insignificant, such as a team member logging onto a laptop, to more significant, such as removal of a virus from a computer. Using technology tools, those activities are narrowed to a few hundred events that are surfaced to the professionals staffing our Security Operations Center (SOC). As a result of their review of these events, dozens of cases are opened daily for additional assessment.

It appears that intruders entered our system on November 12. We now believe that some intruder activity was detected by our computer security systems, logged and surfaced to the SOC and evaluated by our security professionals. With the benefit of hindsight and new information, we are now asking hard questions regarding the judgments that were made at that time and assessing whether different judgments may have led to different outcomes.

We believe that the intruders initially obtained an HVAC vendor's credentials to access the outermost portion of our network. We are still investigating how the intruders were able to move through the system using higher-level credentials to ultimately place malware on Target's point-of-sale registers. The malware appears to have been designed to capture payment card data from the magnetic strip of credit and debit cards prior to encryption within our system.

On the evening of December 12, we were notified by the Justice Department of suspicious activity involving payment cards used at Target stores. We immediately started our internal investigation.

On December 13, we met with the Justice Department and Secret Service. On December 14, we engaged an outside team of experts to lead a thorough forensic investigation.

On December 15, we confirmed that criminals had infiltrated our system, installed malware on our point-of-sale network and potentially stolen guest payment card data. That same day, we removed the malware from virtually all registers in our U.S. stores.

Over the next two days, we began notifying the payment processors and card networks, preparing to publicly notify our guests, and equipping call centers and stores with the necessary information and resources to address our guests' concerns.

Our actions leading up to our public announcement on December 19 – and since – have been guided by the principle of serving our guests. We moved quickly to share accurate and actionable information with the public. When we announced the intrusion on December 19, we used multiple forms of communication, including a mass-scale public announcement, email, prominent notices on our website, and social media.

Additionally, when we subsequently confirmed the theft of certain personal data, we used various channels of communication to notify our guests on January 10.

The breach affected two types of data: payment card data, which affected approximately 40 million guests, and certain personal data, which affected up to 70 million guests. The theft of the payment card data affected guests who shopped at our U.S. stores from November 27 through December 18. The theft of personal data included name, mailing address, phone number or email address, and in many cases, it was partial in nature.



It is difficult to develop an accurate assessment of overlap between these two types of data, due in part to the partial nature of the information related to the file of 70 million individuals. Our analysis indicates there is an overlap of at least 12 million guests in the two populations, and likely more.

### **III. Protecting Our Guests**

From the outset, our response to the breach has been focused on supporting our guests and taking action to further protect them against constantly evolving cyber threats. We are taking a hard look at security across the network. While we don't know everything yet, we have initiated the following steps to further protect our perimeter and better secure our data:

Segmentation. We are increasing the segmentation and separation of key portions of our network by enhancing the protections provided by the firewalls we have in place to limit unauthorized traffic. This is about making it more difficult to move across our network.

Whitelisting. We continue to strengthen our anti-virus tools, and accelerated the installation of a whitelisting solution on our registers. Whitelisting protects guests by detecting malicious applications and stopping them from running on our registers and gives us another tool to prevent malware from taking root and spreading in our environment. This is about limiting what can run on our network.

Authentication. We are strengthening our network perimeter by expanding two-factor authentication for entry into the system. This is about double locking the door.

Beyond these technology responses, we need to ensure the right people, with the right experience, are in the right place. That's why we are also taking a hard look at our organization, with the intention of bolstering our information security structure and practices.

- Earlier this month, Target became the first retailer to join the Financial Services Information Sharing and Analysis Center (FS-ISAC), an initiative developed by the financial services

industry to help facilitate the detection, prevention, and response to cyber attacks and fraud activity. Target was eligible to join the organization because of its financial operations.

During my testimony to Congress in February, I stressed Target's commitment to more coordinated information sharing with law enforcement and others fighting cyber threats, in order to help make our company, partners and guests more secure. Joining the FS-ISAC underscores Target's position that the retail and financial industries have a shared responsibility to collaborate and strengthen protection for American consumers.

- We are accelerating our \$100 million investment in the adoption of chip technology because we believe it is critical to enhancing consumer protections. We have already installed approximately 10,000 chip-enabled payment devices in Target stores and expect to complete the installation in all Target stores by this September, six months ahead of schedule. We also expect to begin to issue chip-enabled Target REDcards and accept all chip-enabled cards by early 2015. As a founding member and steering committee member of the EMV Migration Forum, we will continue to lead the adoption of these technologies across the payment ecosystem.
- We continue to reissue new Target credit or debit cards immediately to any guest who requests one.
- We continue to offer one year of free credit monitoring and identity theft protection to anyone who has ever shopped at our U.S. Target stores. This protection includes a free credit report, daily credit monitoring, identity theft insurance and unlimited access to personalized assistance from a fraud resolution agent.
- We have informed our guests that they have zero liability for fraudulent charges on their cards arising from this incident. To ensure our guests are protected, we continue to

encourage them to monitor their accounts and promptly alert either Target or their issuing bank, as appropriate, of any suspicious activity.

#### **IV. Moving Forward**

For many years, Target has invested significant capital and resources in security technology, personnel and processes. Prior to the data breach, we had in place multiple layers of protection, including firewalls, malware detection software, intrusion detection and prevention capabilities, and data loss prevention tools. We performed internal and external validation and benchmarking assessments. And, in September 2013, our systems were certified compliant with the Payment Card Industry Data Security Standards, meaning that we met approximately 300 independent requirements of the assessment. Yet the reality is that our systems were breached.

To prevent this from happening again, none of us can go it alone. All businesses – and their customers – are facing frequent and increasingly sophisticated attacks by cybercriminals. Protecting American consumers is a shared responsibility and requires a collective and coordinated response. Target remains committed to being part of the solution.

#### **V. Conclusion**

I want to once again say to the Members of this Committee and our guests how sorry we are that this happened. We are determined to get things right. Thank you.

# **APPENDIX E**

## **Evan B. Francen, CISSP CISM**

3992 Spruce Road  
Minnetrista, MN 55375

Phone: 952-250-3486 (Mobile)  
Email: [evan@frsecure.com](mailto:evan@frsecure.com)

### **Personal Profile:**

Results-driven information security executive professional, with demonstrated success employing business, technical, and personal skills in strategic, tactical, and operational information security initiatives.

### **Objective:**

Drive change through close work with corporate/organizational leadership to define, develop, and implement information security strategy that manages acceptable information security risks and aligns with business objectives.

### **Summary of Qualifications:**

- 15 years of progressive technology and information systems security experience
- Skilled in information security strategy, architecture, risk management, and program development
- Experienced with multiple information security regulations and standards including HIPAA, GLBA, Sarbanes-Oxley (SOX), COBIT, ISO 17799/27002, and PCI-DSS
- Designed and delivered numerous enterprise information security training courses
- Strong experience in implementation and support of secure technology within a strict budget
- Proficient in incident response team development and procedures implementation
- Experienced in security policy, guideline, standard and procedure development
- Served as a Subject Matter Expert (SME) in multiple international information security courses
- Proficient in vulnerability, risk, threat analysis and monitoring
- Ability to analyze, respond to, and investigate realized threats swiftly and soundly
- Keen ability in explaining technical information to non-technical personnel in all levels throughout the organization
- Ability to design and manage projects effectively, within budget and on time
- Effective negotiation skills with both internal customers, and external vendors

### **Professional Certification and Membership:**

- Certified Information Systems Security Professional, since February 2005 (CISSP)
- Certified Information Security Manager, since June 2008 (CISM)
- Cisco Certified Network Professional, 2000 – 2006 (CCNP)
- Microsoft Certified Systems Engineer, 1998 – 2003 (MCSE)
- Information Systems Audit and Control Association – member (ISACA)
- Information Systems Security Association – member (ISSA)

### **Professional Experience:**

**FRSecure LLC – Minnetrista, MN**

**January, 2008 – Present**

#### **President**

- Co-founded FRSecure LLC; a full-service information security consulting company created out of the desire to help organizations understand, design, implement, and manage best-in-class information security solutions.
- Developed a proprietary information security assessment methodology, using the ISO 17799:2005 (27002) international standard as a framework, to accurately represent the risks of unauthorized information disclosure, modification and destruction.
- Reviewed the information security programs of and provided information security consulting services to more than 50 companies ranging in size from 3 employees to more than 54,000 employees between mid-2009 and present.
- Designed the services that comprise FRSecure's strategic and tactical service offerings, including the Enterprise Information Security Assessment ("EISA"), Enterprise Information Security Program Development ("EISD"), Enterprise Information Security Management ("EISM"),

Information Security Incident Response, Penetration Testing, Business Continuity Planning, Enterprise Information Security Training (“EIST”), and Legal Expert Witness/Testimony.

**Breachblog.com – Minneapolis, MN                      August, 2007 – February, 2009 and June, 2010 - Present**  
**Security Researcher and Author**

- Founded Breachblog.com out of my passion to research, report facts, and provide opinion on information security breaches concerning personally identifiable information.
- Researched and reported on more than 600 breaches over the course of 18 months
- Increased daily reader email subscriptions from one to more than 900
- Provided interviews and documentation to numerous news outlets

**Eisai, Inc. (Formerly MGI PHARMA – Bloomington, MN                      October, 2006 – February, 2009**  
**Director of Information Security and Architecture**

- Designed and implemented MGI PHARMA’s first formal information security program based on a thorough analysis of risk to MGI’s information resources, industry standard best practices and various governmental rules and regulations including Sarbanes-Oxley (SOX) and FDA 21 CFR Part 11.
- Led numerous information security control projects including policy, standards and procedures development, training & awareness, laptop encryption, data in transit and at rest encryption, network access control, automated patching, secure configuration standards, internal and external security audits, and disaster recovery planning.
- Provide direction to a highly skilled team of engineers that substantially improved MGI’s network and server infrastructure by implementing and supporting scalable and highly-available solutions
- Designed and implemented MGI PHARMA’s first formal disaster recovery program covering four geographically dispersed sites, based on a thorough analysis of critical MGI information resources as determined by our Business Impact Analysis (BIA)
- Responsible for the information security and architecture annual operating plans (budgets)

**eLoyalty Corporation (ELOYY) – Eden Prairie, MN                      January, 2006 – October, 2006**  
**Director of Information Security**

- Developed, implemented, and supported eLoyalty’s first formal information security program, a progressive information security life-cycle program that met the needs of our business, customers, and various governmental and industry regulations
- Created, implemented, and enforced various information security and operational policies including the Managed Services Information Security Policy, Data Classification Policy, Incident Response and Security Training and Awareness Policy
- Oversaw risk management, penetration testing, vulnerability scanning and other information security audit/test related projects
- Designed, installed, and oversaw the enterprise-class intrusion detection/prevention architecture, monitoring traffic across 100+ VLANs, including incident response.
- Led eLoyalty’s first SAS 70 Type I engagement from preparation through to final report
- Coordinated and communicated all types of information security projects with people at all levels of multiple organizations, from end-user to “C-Level” executives

**UnitedHealth Technologies (UNH) – Plymouth, MN                      October, 2005 – January, 2006**  
**Information Security Project Manager (consultant)**

- Technical project manager dedicated to a project to deploy full-disk encryption to 46,000 laptops across six business divisions within UnitedHealth, to address data at rest HIPAA concerns.
- Coordinated all aspects of the project, including vendor selection, testing, deployment strategies, end-user support, and back-end architecture design

## **Professional Experience (continued):**

### **U.S. Bank (USB) – Saint Paul, MN**

**Data Security Consultant III-Threat and Vulnerability**      **March, 2005 – October, 2005**

- Developed, implemented and supported enterprise-level solutions created to reduce the impact of realized threats, and decrease the number of vulnerabilities in an environment that spans more than 100,000 computers and devices.
- Responded to, investigated, and provided remediation to a wide variety of realized security incidents, including distributed denial of service (DDoS) attacks, attempted network intrusions and breaches, phishing and Internet fraud attacks, and unauthorized access attempts among many others
- Lead Threat and Vulnerability team projects to address the specific security needs of the organization, including PCI-DSS compliant auditing, logging and remediation for servers, and GLBA-compliant intrusion detection monitoring of host intrusion detection systems (HIDS) and network intrusion detection systems (NIDS)
- Lead detailed forensic investigations into employee security incidents including embezzlement, ethics violations, computer misuse, Internet abuse, email misuse, and other technical information security policy violations.
- Consulted with all levels of the organization in regards to security issues, interpretations and reviews.

### **Corel Corporation (CREL, formerly Jasc Software, Inc.) – Eden Prairie, MN**

**Information Security/Network Services Manager**      **March, 2000 – March, 2005**

- Designed, developed, implemented and managed all aspects of technical and non-technical security within the network management facilities and IP network infrastructure including data center, management center, and administrative areas
- The department proactively managed in excess of 150 production Windows servers, co-located servers in remote data centers, Internet accessible Web servers, a Fiber Channel Storage Area Network, clustered SQL database servers, 802.11 wireless access points, a DS3 Internet data circuit, Cisco firewalls, Cisco routers, and Cisco switches among many other services and devices.
- Started a company-wide communication initiative in an effort to provide both formal and informal dialog between Information Services and the department managers with the ultimate goal of providing better service to our customers
- Our team planned, tested, piloted, rolled-out, and documented a successful migration from a Windows NT 4 based infrastructure to Windows 2003 within budget and on time
- Developed an all-encompassing and fully redundant alerting and monitoring architecture utilizing local and off-site sensors.
- Maintained 99.9989% availability while providing for 3.6 billion web hits, 122 million trial downloads, and 556 thousand ecommerce orders through our Internet architecture
- In early 2004, the team successfully protected all internal services, and the mail server itself from over 3 million incoming, daily emails at the height of the W32.Mydoom.A worm outbreak. A new architecture was designed out of this process that will minimize, if not eliminate, the negative impact of future email worm outbreaks
- Responsible for analyzing, reporting on, and effecting change in the state of Internet and local network security
- Organize, provide direction to, and mentor a team of highly qualified technical individuals
- Responsible for the 1.8 million dollar Information Services non-capital budget, purchasing, and external vendor relationships

### **KRS Computer & Business School – Bloomington, MN**

**Consultant - Lead Cisco CCNP Instructor**      **December, 1999 – March, 2001**

### **Valley View Microsystems – Eden Prairie, MN**

**Senior Consultant**      **November, 1997 – March, 2000**

**Professional Experience (continued):**

**Network Computing Solutions – Minneapolis, MN**  
**Lead Information Security Consultant**

**January, 1993 – November, 1997**

**Education:**

- University of Minnesota, College of Liberal Arts 1988 – 1991  
Major: Geology  
Varsity “M” Letter Winner in Men’s Swimming





**EVAN B. FRANCEN, CISSP CISM**  
President of FRSecure LLC  
"Information Security is good business"

Evan Francen is a passionate information security expert who serves businesses of all sizes, in all industries by cooperatively solving the complex issues surrounding information security. He is considered to be an "information security evangelist".

Prior to establishing FRSecure, Evan spent more than 15 years as a leading information security professional and corporate leader in both private and public companies. He is well-versed in governmental and industry-specific regulations, standards and guidelines including ISO/IEC 27002 (17799:2005), HIPAA, GLBA, PCI-DSS, FDA CFR Part 11, SOX and COBIT, but also understands the intricacies in aligning compliance with business objectives. Most recently, and prior to establishing FRSecure LLC, Evan established the formal information security programs for four publicly-traded companies; Corel Corporation (CREL), Mattersight Corporation (MATR), MGI Pharma(MOGN) and Eisai Ltd (TSE).

Evidence of Evan's true passion for information security can be found in his many writings on the subject. He has written in excess of 700 information security articles, and developed and taught numerous information security courses. He has also been featured in radio interviews with noted organizations such as BBC Radio (UK), and has provided expert information security advice in legal proceedings.

Information security professionals need to stay current in order to remain effective. Evan is an active participant in many information security organizations including the International Information Systems Security Certification Consortium (ISC<sup>2</sup>), the Information Systems Audit and Control Association (ISACA), and the Information Systems Security Association (ISSA) among others. Evan also holds the "Gold Standard" Certified Information Systems Security Professional (CISSP) and Certified Information Security Manager (CISM) certifications.

Information security is a complex and holistic discipline that can be confusing to people who are not dedicated to it. Evan's keen ability to explain technical information to non-technical personnel in all levels throughout an organization, his unique sense of humor, and his "tell it like it is" demeanor, gets the point across and produces results for FRSecure clients.



952-442-1709  
info@frsecure.com  
150 Pioneer Trail #125  
Chaska MN 55318

# **APPENDIX F**

## ***William E. McCracken***

6 Holly Drive □ Warren, New Jersey 07059

Mobile Phone: 908.755.4640 □ E-mail: wemsh42@gmail.com

---

### **PRESIDENT/CEO**

#### **QUALIFICATIONS PROFILE**

Accomplished *President/CEO* with exceptional corporate governance and operational leadership history, experience with directing senior management teams, and record of developing and executing business strategy. Inspirational leader and motivator with reputation for establishing and sustaining collaborative senior leadership, distinguished service on boards of directors, development of committee partnerships and alliances, and leading security and corporate- governance management initiatives. Creative marketing visionary with unrelenting focus on industry innovation, quality, and performance excellence.

#### **CORE COMPETENCIES**

- *Global Operations Management, Senior Team Leadership & Performance Management*
- *Security Management, IT Governance, Infrastructure & Configuration Management*
- *Application Performance Optimization, Change Management*
- *Information Governance, IT Asset Management, Database Management*
- *Project & Portfolio Management, Financial Management*
- *Marketing, Sales, Service, Support, Manufacturing, & Distribution*

#### **PROFESSIONAL EXPERIENCE**

##### **EXECUTIVE CONSULTING GROUP, LLC, Warren, New Jersey, 2002 - Present**

*(National business consulting firm.)*

*President/Chief Executive Officer*

- Traveling nationally, consulting with *Fortune 500* companies, and recommending corporate governance and business development strategy.

##### **CA TECHNOLOGIES, New York, New York, 2005 - 2012**

*(Global Fortune 500 software company providing corporate, IT management, and security services.)*

*Chief Executive Officer, 2010 - 2012*

*Executive Chairman of Board of Directors, 2010*

*Chairman of Board of Directors, 2007 - 2010*

*Director, Board of Directors/Chair of the Special Litigation Committee, 2005 - 2007*

- Oversaw global operations, directed senior leadership team, drove marketing, development, and distribution, and support to a global *1000* client base, and *delivered \$4.2 billion to \$4.7 billion in annual revenue*.
- Championed/led integration of new cloud-based technology into software service offerings, created new profit stream, and *substantially enhanced business growth*.

##### **MDU RESOURCES GROUP, INC., Bismarck, North Dakota, 2013 - Present**

*(National gas & electric utility, & construction services provider.)*

*Board of Directors Member*

*Nominating & Governance Committee Member*

*Compensation Committee Member*

##### **IKON OFFICE SOLUTIONS, INC., Malvern, Pennsylvania, 2003 - 2008**

*(Multi-billion-dollar national printing and office services solution provider.)*

*Board of Directors Member*

*Audit Committee & Investment & Strategy Committee Member*

**PROFESSIONAL EXPERIENCE****IBM, 1965 - 2001****General Manager, Global PC Division, 1998 - 2001**

- Oversaw *Printing Systems Division*, directed research, development, marketing, distribution, and service operations, facilitated delivery of large-scale printing solutions to global 3000 companies, and ***drove a multi-billion-dollar revenue stream.***
- Directed senior leadership and cross-functional team, oversaw development and deployment of hardware and software technology, drove profitable distribution of commercial high-speed color printing equipment and software systems, and ***expanded business footprint and market share.***

**Worldwide Management Council Member, 1995 - 2001**

- Appointed to serve on a 27-member prestigious senior executive council by the *IBM Chairman*.

**General Manager, Marketing, Sales, & Distribution Division, 1994 - 1998****President, EMEA, Asia Pacific Division, 1993 - 1994**

- Led worldwide *Sales, Marketing, and Distribution* initiatives for *IBM PC Division*, recruited/managed 40 to 50-member executive team, and ***delivered a multi-billion-dollar sales and distribution performance.***

**General Manager, PC Business Sector, Europe, Middle East, & Africa, 1991 - 1993**

- Oversaw *EMEA Marketing, Service, Support, Manufacturing, and Distribution* operations, directed 20-member senior executive team, and successfully delivered *PC* software and hardware services to a lucrative commercial and retail customer base.
- Championed and led development, production, and distribution of low-cost *PC* systems, expanded market reaches, and ***substantially increased sales and profitability.***

**BOARD MEMBERSHIPS AND RECOGNITIONS**

- *The National Association of Corporate Directors, National Board of Directors Member, 2009 - Present*
- *Chairman's Forum, Chairman, 2007 - Present*
- *Washington Board of Trade and NACD Forum, 2015, Presenter on Cyber Security*
- *NACD National & Regional Forums on Corporate Governance, 2015, Presenter*
- *NACD Blue Ribbon Commission, Co-Chairman, 2015, "The Board and Long-Term Value Creation"*
- *NACD Blue Ribbon Commission, Co-Chairman, 2012, "The Diverse Board"*
- *NACD Blue Ribbon Commission, Commissioner, 2009, "Risk Governance"*
- *NACD Directorship Magazine Top 100 Most Influential People in the Boardroom*
- *Numerous CNBC Closing Bell Appearances*
- *Corporate Governance & Business, Presenter, Columbia, Harvard, NYU, and Stanford Universities*

**EDUCATION****SHIPPENSBURG UNIVERSITY, Shippensburg, Pennsylvania**

- *Bachelor of Science Degree, Physics, 1964*
- *Minor: Mathematics*

## ***William E. McCracken***

6 Holly Drive □ Warren, New Jersey 07059

Office Phone: 908.755.4640 □ E-mail: [wemsh42@gmail.com](mailto:wemsh42@gmail.com)

---

### ***BIO***

Between 2010 and 2012 *William E. McCracken* served as Chief Executive Officer for CA Technology, a Fortune 500 information management and security software leader. He served as a member of CA's Board of Directors between 2005 and 2012, chaired the Special Litigation Committee from 2005 to 2007, and held non-executive and executive chairman roles from 2007 to 2010. Prior to that, Bill was employed by IBM for 30+ years where he was General Manager of the EMEA PC Business Unit, President of EMEA/Asia Pacific PC Business Unit, and later transitioned to the General Manager of the Global PC Division and assumed responsibility for sales, marketing, and distribution.

Currently Bill is Chairman of The Board at the Millstein Center at Columbia Law School for Global Markets and Corporate Ownership he serves on the Board of National Association of Corporate Directors, and recently co-chaired the 2015 NACD Blue Ribbon Commission that produced a definitive study on "The Board and Long-term Value Creation". He also co-chaired the 2012 Blue Ribbon Commission on Diversity and was a Commissioner on the 2009 Blue Ribbon Commission on Risk Governance, which focused on balancing risk and reward. Bill also serves as Chairman of the NACD's Chairman's Forum. A frequent presenter for NACD National and Regional Forums on Corporate Governance and cybersecurity, Bill has also addressed Harvard, Columbia, NYU, and Stanford University audiences. In addition he has logged numerous appearances on CNBC Closing Bell, and CNBC Asia.

In 2003, Bill was elected to a 5-year term on the Board of Ikon Office Solutions and has served on the Audit and Investment & Strategy Committees. He currently is a member of the Board of Directors of MDU Resources Group, Inc. and serves on its Nominating Governance and Compensation Committees.

A seasoned *CEO* with three decades of senior leadership experience, Bill has been recognized as an industry leader and subject matter expert on corporate governance and cybersecurity. He has also been a key player in the development of corporate board-of-directors roles and an outspoken industry advocate and change agent. He has been a frequent presenter to corporate directors and academic audiences, championed the need for change, and pioneered development of governance guidelines for the corporate environment. In recent years, Bill has devoted himself to providing governance leadership and direction in a diversity of academic, board leadership, and corporate scenarios.

# **APPENDIX G**

Interviewee	Title ^^
Roxanne Austin	Member of the Board of Directors and named defendant
Tim Baer	Executive Vice President and Chief Legal Officer and Corporate Secretary
Doug Baker	Member of the Board of Directors and named defendant
Tricia Bartylla	Director of Assurance
Dave Baumgartner	Current Vice President, Cyber Security
Brenda Bjerke	Senior Director of TIP, Chief Privacy Officer, and HIPAA Security/Privacy Officer
Marc Black	Director of Emerging Financial Services
Bob Blank	Engineering Consultant, Security Engineering team within TTS
Brian Bobo	Manager of the Security Operations Center until October 2013
Ralph Boelter	Vice President, Corporate Security
Adrian Butler	Senior Director, Infrastructure Planning and Security
Steven Chin	Senior Engineer in Client Technologies Point of Sale Hardware Engineering
Calvin Darden	Member of the Board of Directors and named defendant
Fritz Debrine	Director, Enterprise Engineering Server, Network & Client
Henrique De Castro	Member of the Board of Directors and named defendant
Bob DeRodes	Interim Chief Information Officer and Executive Vice President
John Deters	Engineering Consultant, Point of Sale Hardware
Peter Dowd	Director, Enterprise Engineering Software Technologies
Sarah Engstrom	Senior Group Manager, Awareness & Intake team within TIP
Janine Foster	Senior Group Manager, Canada Privacy, Guest Data Lifecycle, and US Privacy within TIP
Erin Getty**	Manager of Risk Assessment
Paul Gunderson	Manager of Vulnerability Management
Al Hannagan	Senior Vice President of Enterprise Risk Management and Information Security at Trustwave Holdings, Inc.
Jadee Hanson	Senior Group Manager, Consulting and Vendor Assessments
Tony Heredia	Vice President, Strategy and Operations
Jeff Holschuh	Manager of Active Directory, Access and Database Management within TTS
Doug Hunter	Lead audit partner on the Target engagement from Ernst & Young
Beth Jacob	Target's Chief Information Officer and named defendant
James Johnson	Former member of the Board of Directors and named defendant
Scott Kennedy	President, Target Financial and Retail Services
James Kist	Lead assessor for Target PCI DSS assessment for Trustwave Holdings, Inc.
Carter Leuty	Vice President of Law
Marek Lewicki	Senior Investigative Consultant for Information Security Investigations
Mike Lexa	Group Manager, IT Security and Compliance
Terry Mackin	Senior Group Manager, Point of Sale Hardware within TTS
Jeff Mader	Vice President, Infrastructure and Security
Brad Maiorino	Current Senior Vice President and Chief Information Security Officer
Garrett Markin**	Analyst performing risk assessments for TIP

Matt McCabe	Lead Engineering Consultant
Paul McCabe	Senior Group Manager, Global Investigations, Information Security Investigations
Gordon McCarty	Lead Technical Architect within TTS
Jeremy Milburn	Group Manager, Audit Support, Compliance, Risk Assessments and Risk Treatment
Mary Minnick	Member of the Board of Directors and named defendant
Anne Mulcahy	Member of the Board of Directors and named defendant
John Mulligan	Chief Financial Officer, Interim Chief Executive Officer from May through August 2014, and named defendant
Chris Novak	Target's PCI Forensic Investigator after the breach
Jim Ostergaard	Senior Director, Solution Engineering Group
Brent Pack	Senior Investigative Consultant, Information Security Investigations
David Pankratz	Senior Engineer on the POS Hardware Engineering team
Greg Patyk	Senior Manager, Global & Information Security Investigations
Todd Peterson	Analyst, Incident Response within TIP
Joe Pletsch	Lead Technical Architect
Jason Reasoner	Senior Engineer, Client Technologies Mobility Team within TTS
Derica Rice	Member of the Board of Directors and named defendant
Jackie Hourigan Rice	Current Executive Vice President and Chief Risk and Compliance Officer
Jonathan Ruud	Engineer and Investigator within the Security Operations Center
Kenneth Salazar	Member of the Board of Directors and named defendant
Mike Salters	Group Manager, IT Security - Operations & Run
Ann Scovil	Vice President of Assurance, Risk, and Compliance, Chief Compliance Officer, and Chief Audit Officer
Terry Scully	Former President, Financial and Retail Services
Melissa Seebeck	Senior Group Manager, Cyber, Incident Response, Policy, and Project Support
Scott Siebert	Group Manager, Security Program and Process
Gregg Steinhafel	Chairman of the Board, Chief Executive Officer, and President and named defendant
John Stumpf	Member of the Board of Directors and named defendant
Ann Teynor	Senior Counsel, Law
Erik Thoreson	Senior Engineer in IT Applications Security within TTS
Solomon Trujillo	Former member of the Board of Directors and named defendant
Nhila Vang	Engineering Consultant, Security Engineering Build team
Vicki Wold	Senior Group Manager, IT Security and Planning within TTS
Consulting expert retained by outside counsel	

^^ Unless otherwise noted, the title listed is at the time of the data breach

\*\* Interviewee was interviewed SLC counsel only.



# **APPENDIX H**

TARGET BOARD OF DIRECTORS

COMMITTEE ASSIGNMENTS AT THE  
TIME OF THE DATA BREACH

**Audit Committee**

Roxanne Austin, **Chair**  
Mary Minnick  
Derica Rice  
Anne Mulcahy

**Nominating and Governance  
Committee**

Anne Mulcahy, **Chair**  
Douglas Baker  
Calvin Darden  
Solomon Trujillo  
Kenneth Salazar

**Compensation Committee**

James Johnson, **Chair**  
Calvin Darden  
John Stumpf  
Douglas Baker

**Finance Committee**

Derica Rice, **Chair**  
Roxanne Austin  
John Stumpf  
Henrique De Castro

**Corporate Responsibility  
Committee**

Solomon Trujillo, **Chair**  
Calvin Darden  
Henrique De Castro  
James Johnson  
Mary Minnick  
Kenneth Salazar (Chair-elect)

